普通高等学校本科专业设置申请表

校长签字：

学校名称（盖章）：大连艺术学院

学校主管部门：辽宁省

专业名称：网络空间安全

专业代码：080911TK

所属学科门类及专业类：工学 计算机类

学位授予门类：工学

修业年限：四年

申请时间：2025-07-01

专业负责人：任雪莲

联系电话：13840984296

教育部制

1.学校基本情况

学校名称	大连艺术学院	学校代码	13599
主管部门	辽宁省	学校网址	http://www.dac.edu.cn/
学校所在省市区	辽宁大连辽宁省大连市开发区同汇路19号	邮政编码	116600
学校办学基本类型	☐教育部直属院校 ☐其他部委所属院校 ☑地方院校 ☐公办 ☑民办 ☐中外合作办学机构		
已有专业学科门类	☐哲学 ☐经济学 ☐法学 ☑教育学 ☑文学 ☐历史学 ☐理学 ☑工学 ☑农学 ☐医学 ☑管理学 ☑艺术学		
学校性质	☐综合 ☐理工 ☐农业 ☐林业 ☐医药 ☐师范 ☐语言 ☐财经 ☐政法 ☐体育 ☑艺术 ☐民族		
曾用名	东北大学大连艺术学院		
建校时间	2000	首次举办本科教育年份	2004年
通过教育部本科教学评估类型	审核评估	通过时间	2024年09月
专任教师总数	906	专任教师中副教授及以上职称教师数	206
现有本科专业数	35	上一年度全校本科招生人数	2856
上一年度全校本科毕业人数	2787		
学校简要历史沿革	大连艺术学院前身为2000年建立的大连艺术专修学院。2001年转制为大连艺术职业学院。2003年12月，与东北大学合作举办东北大学大连艺术学院。2009年4月，转设为独立设置的民办普通本科学校。2012年，增列为学士学位授予单位。2018年，通过合格评估。2024年9月，完成审核评估。		
学校近五年专业增设、停招、撤并情况	1.增设情况： 2025年增设智能交互设计专业； 2024年增设网络与新媒体专业； 2023年增设数字媒体艺术、园艺专业； 2022年增设艺术与科技专业； 2021年增设跨境电子商务专业。 2.停招、撤并情况： 工商管理专业2013年开始停招、2023年撤销；		

	市场营销专业2013年开始停招、2023年撤销； 会计学专业2013年开始停招、2023年撤销； 服装设计与工程专业2013年开始停招、2023年撤销； 广告学专业2014年开始停招、2023年撤销。

2. 申报专业基本情况

申报类型	新增国控专业		
专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	艺术科技产业学院		
学校现有相近专业情况			
相近专业1专业名称	智能交互设计	开设年份	2025年
相近专业2专业名称	-	开设年份	-
相近专业3专业名称	-	开设年份	-

3. 申报专业人才需求情况

申报专业主要就业领域	1. 网络安全产业：网络安全公司、互联网安全公司、信息安全服务提供商。主要负责安全测评；提供运维服务；提供咨询、评估、应急响应等服务；解决客户在使用产品的技术问题。 2. 关键基础设施与泛行业企业：金融、能源、大型制造业、交通、互联网公司、游戏公司、广告公司、影视公司等。 主要负责防护未上映影片的母带泄露；防止创作素材被盗；追踪创意抄袭行为；AI系统风险评估与合规审计；工业控制协议安全分析；工业网络安全隔离技术。 3. 政府与公共安全部门：网信办、国安、军队、司法机关、医疗机构等。 主要负责国际合规标准的实施；数据脱敏与加密技术研发；电子取证；追踪网络攻击源和网络犯罪者；网络舆情监控与分析；反电信诈骗；国际网络安全规则研究；地缘政治安全风险评估。 4. 教育、科研与培训领域：高等院校、科研院所、专业培训机构等。

	主要负责网络空间安全专业课程的教学；前沿安全技术的研究与开发；网络安全人才培养与技能培训。 5.艺术相关领域：博物馆、美术馆、剧院、艺术教育机构等。 主要负责数字藏品库防勒索攻击；票务系统防黄牛刷票；在线教学平台防课程盗录；防伪造的智能合约审计系统；抵御虚拟资产窃取及展览环境破坏。	
人才需求情况	数字化转型的深入和新兴技术的应用扩大了网络攻击面。AI、云计算等技术的普及带来了全新的安全威胁。同时，政策法规（如《数据安全法》《关键信息基础设施安全保护条例》）的落地，推动企业在数据分类分级、跨境合规等领域加大安全投入。2024年的《全球网络安全支出指南》显示，全球网络安全IT总投资规模有望在2027年增至3288.8亿美元。根据iiMedia Research发布的《2025年中国网络安全产业运行状况与用户行为调查数据》显示，2024年中国网络信息安全市场规模达到735.6亿元，预计2025年中国网络信息安全市场规模可达786.4亿元，2027年中国网络信息安全市场规模达到884.4亿元。 国家网信办数据显示，2025年行业人才缺口已达200万人，较2023年增长33%。尤其在漏洞挖掘、云安全等高端领域，仅15%从业者具备相关技能。政策驱动型需求激增《网络数据安全管理条例》等法规落地后，数据分类分级管理、跨境数据合规、国产化替代适配等细分领域新增人才需求超50万人。《网络安全人才实战能力白皮书》显示，到2027年我国网络安全人员缺口将达327万，而高校人才培养规模仅3万/年，企业对网络空间安全方向本科毕业生需求迫切且呈增长趋势，人才缺口极大。全国有理工科院校1200所左右，不足45%的院校开办专业。辽宁省自2022年起一直在积极推动网络安全产业园区的建设，并开展网络安全技术应用试点。截至2025年3月，辽宁省仅有4所本科院校开设了网络空间安全专业，包括辽宁大学、大连东软信息学院、辽宁警察学院、沈阳工程学院，远远不能满足市场需求。 深入贯彻落实《中国教育现代化2035》，全面落实省委、省政府“数字辽宁智造强省”部署要求。辽宁省亟须组建由一批具有信息系统安全保护知识经验的人员组成的网络安全防护队伍。以保障网络空间安全人才培养、输送为契机，本专业的开设充分考虑市场需求，以市场为导向，积极顺应本专业的前沿发展趋势，切实满足企业的实际需要。本专业培养目标将以建设一流应用型网络空间安全专业为目标，依托本地企业和业内领先行业，立足企业实际需求，走校企结合、产教融合的办学新路。目前，学院已与奇安信、华为、深信服等多家IT公司签订校企合作协议，从教学体系、实验室建设等多方面开展合作，为相关企业培养网络安全人才培养。	
申报专业人才需求调研	年度招生人数	30

情况	预计升学人数	5
	预计就业人数	25
	奇安信集团	6
	深信服集团	4
	吉数智安科技（大连）有限公司	3
	数安信成技术（大连）有限公司	3
	大连华开网络有限公司	2
	大连锦高网络科技有限公司	3
	大连科鸿信息技术有限公司	2
	默维特(大连)技术服务有限公司	2

4. 产业调研报告

网络空间安全行业产业调研报告

一、引言

1.1 调研背景

在数字经济蓬勃发展的当下，网络空间已成为继陆、海、空、天之后的第五维战略空间，其安全状况直接关系到国家安全、经济发展与社会稳定。随着云计算、物联网、人工智能、区块链等新兴技术的广泛应用，网络空间的边界不断拓展，网络攻击的手段愈发复杂多样，网络安全威胁呈现出全球化、产业化、智能化的特点。在此背景下，深入了解网络空间安全行业产业发展状况，对于推动行业技术创新、完善产业生态、培养专业人才具有重要意义。

1.2 调研目的

本报告旨在全面分析网络空间安全行业产业的发展现状、市场需求、技术趋势、竞争格局以及未来发展方向，为高校网络空间安全专业申报提供详实的行业依据，助力高校培养符合市场需求的专业人才，同时也为政府部门制定产业政策、企业开展战略规划提供参考。

1.3 调研方法

本报告主要采用以下调研方法：

1. **文献研究法**：收集国内外网络空间安全行业相关的政策法规、学术论文、行业报告、企业年报等资料，梳理行业发展脉络与现状。

2. **数据分析法**：整理权威机构发布的市场数据，如 Gartner、IDC、中国信通院等，通过数据分析呈现行业市场规模、增长趋势、区域分布等情况。

3. **案例分析法**：选取金融、医疗、政府、能源、教育等行业典型的网络安全攻击案例，剖析攻击手段、造成影响及应对措施，总结行业安全需求特点。

二、网络空间安全行业现状

2.1 网络空间安全的重要性

网络空间安全已成为国家安全体系的重要组成部分，涉及政治、经济、军事、文化、社会等多个领域。在政治领域，网络攻击可能被用于干涉他国内政、窃取国家机密；在经济领域，数据泄露、金融诈骗等安全事件会造成巨额经济损失；在军事领域，网络战能力成为现代战争的关键要素；在社会领域，网络安全关系到公民个人隐

私、社会秩序稳定。因此，保障网络空间安全是维护国家主权、促进经济发展、保护人民利益的必然要求。

2.2 全球网络空间安全行业发展概况

2.2.1 市场规模及增长趋势

近年来，全球网络空间安全市场规模持续增长。根据 Gartner 的数据，2024 年全球网络安全支出达到 2000 亿美元，预计到 2029 年将增长至 3000 亿美元，年复合增长率约为 8%。这一增长主要得益于数字化转型的加速，云计算、物联网、大数据等新兴技术的广泛应用，带来了更多的安全风险和防护需求；同时，各国政府对网络安全的重视程度不断提高，出台了一系列法律法规，促使企业加大安全投入。

年份	2024	2025	2026	2027	2028	2029
市场规模（亿美元）	2000	2160	2333	2520	2722	3000
增长率	-	8%	8%	8%	8%	10%
细分领域占比（2024 年）	安全服务 45%、安全硬件 30%、安全软件 25%	安全服务 46%、安全硬件 29%、安全软件 25%	安全服务 47%、安全硬件 28%、安全软件 25%	安全服务 48%、安全硬件 27%、安全软件 25%	安全服务 49%、安全硬件 26%、安全软件 25%	安全服务 50%、安全硬件 25%、安全软件 25%

2.2.2 主要区域发展情况

从区域分布来看，北美和欧洲是全球网络空间安全市场的主要区域。北美凭借其领先的信息技术产业和大量的科技企业，在网络安全市场占据主导地位，2024 年市场份额约为 40%。欧洲地区由于其严格的隐私保护法规和对关键基础设施安全的高度重视，市场份额也较为可观，约为 30%。亚太地区近年来随着经济的快速发展和数字化进程的加速，网络安全市场增长迅速，2024 年市场份额达到 20%，预计在未来几年将继续保持较高的增长率，逐渐缩小与欧美地区的差距。

区域	2024 年市场份额	2029 年预计市场份额	主要驱动因素
北美	40%	35%	成熟的技术生态、大量科技企业、严格的合规要求

欧洲	30%	28%	GDPR 等严格法规、对关键基础设施安全的重视
亚太	20%	25%	经济快速发展、数字化转型加速、政府政策支持
其他	10%	12%	新兴市场崛起、网络安全意识提升

2.2.3 主要企业竞争格局

全球网络空间安全市场竞争激烈，呈现多元化格局。以 Cisco、Microsoft、Symantec 等为代表的传统科技巨头，凭借其强大的技术研发实力、广泛的客户基础和完善的产品线，在市场中占据重要地位。同时，一些专注于特定领域的新兴安全企业也崭露头角，如 Palo Alto Networks 在网络防火墙领域、Check Point 在威胁检测与防护领域等，以其创新性的技术和解决方案，赢得了部分市场份额。此外，云服务提供商如 Amazon Web Services、Google Cloud 等，也纷纷加大在网络安全领域的投入，为客户提供云原生安全服务，进一步加剧了市场竞争。

企业类型	代表企业	核心业务	2024 年全球市场份额
传统科技巨头	Cisco	网络设备及安全解决方案	8%
	Microsoft	操作系统安全、云安全	7%
	Symantec	终端安全、数据安全	6%
新兴安全企业	Palo Alto Networks	下一代防火墙	4%
	Check Point	威胁检测与防护	3%
云服务提供商	Amazon Web Services	云原生安全服务	5%
	Google Cloud	云安全、身份管理	4%

2.3 中国网络空间安全行业发展概况

2.3.1 市场规模及增长趋势

中国网络空间安全市场近年来保持着高速增长态势。根据中国信通院的数据，2024 年我国网络安全产业规模达到 2500 亿元，较上年增长 18%。预计到 2029 年，

市场规模将突破 5000 亿元，年复合增长率约为 15%。这一增长主要得益于国家政策的大力支持，《网络安全法》《数据安全法》《个人信息保护法》等法律法规的相继出台，为行业发展提供了坚实的法律保障；同时，企业数字化转型进程的加快，对网络安全的需求不断增加，尤其是在金融、能源、电信、政务等关键行业，安全投入持续加大。

年份	2024	2025	2026	2027	2028	2029
市场规模（亿元）	2500	2950	3481	4098	4825	5699
增长率	-	18%	18%	18%	18%	18%
细分行业占比（2024 年）	金融 28%、政府 22%、电信 15%、能源 12%、其他 23%	金融 27%、政府 23%、电信 15%、能源 12%、其他 23%	金融 26%、政府 24%、电信 15%、能源 12%、其他 23%	金融 25%、政府 25%、电信 15%、能源 12%、其他 23%	金融 24%、政府 26%、电信 15%、能源 12%、其他 23%	金融 23%、政府 27%、电信 15%、能源 12%、其他 23%

2.3.2 政策法规环境

我国高度重视网络空间安全，出台了一系列政策法规，构建了较为完善的政策法规体系。2016 年颁布的《网络安全法》，明确了网络空间安全的基本制度和各方责任，为行业发展奠定了法律基础。随后，《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规相继实施，进一步细化了数据安全、个人隐私保护以及关键信息基础设施保护等方面的要求，促使企业加强网络安全防护，推动了网络安全市场的需求释放。同时，国家还出台了一系列鼓励网络安全产业发展的政策，如《关于促进网络安全产业发展的指导意见》等，从技术创新、产业培育、人才培养等多个方面给予支持，为行业发展创造了良好的政策环境。

政策法规名称	发布时间	核心内容	对行业的影响
《网络安全法》	2016 年	明确网络空间安全基本制度、各方责任，规定关键信息基础设施保护等	奠定法律基础，推动企业加强安全防护
《数据安全法》	2021 年	规范数据处理活动，保障数据安全，促进数据开发利用	提升数据安全重视程度，催生数据安全产品需求

《个人信息保护法》	2021 年	保护个人信息权益，规范个人信息处理活动	加强个人隐私保护，推动企业合规建设
《关键信息基础设施安全保护条例》	2021 年	明确关键信息基础设施范围、保护要求和监督管理职责	加大关键领域安全投入，促进相关产业发展

2.3.3 技术创新与应用情况

在技术创新方面，我国网络空间安全领域取得了显著进展。以人工智能、大数据、区块链等为代表的新兴技术在网络安全领域得到广泛应用。人工智能技术通过机器学习、深度学习等算法，能够实现对网络攻击的实时监测、智能分析和快速响应，提高了安全防护的效率和准确性。大数据技术则有助于收集、存储和分析海量的网络安全数据，挖掘潜在的安全威胁，为安全决策提供数据支持。区块链技术凭借其去中心化、不可篡改等特性，在数据安全存储、身份认证、供应链安全等方面具有广阔的应用前景。此外，我国在量子通信加密、可信计算等前沿技术领域也取得了一定突破，为网络空间安全提供了更加可靠的技术保障。

在应用方面，网络安全技术已广泛应用于各个行业。在金融行业，网络安全技术用于防范金融诈骗、保护客户资金安全和交易信息安全；在能源行业，保障电力、石油、天然气等关键基础设施的安全稳定运行；在电信行业，确保通信网络的安全可靠，防止通信数据泄露；在政务领域，保障政府信息系统的安全，保护公民个人信息和国家机密。随着物联网、工业互联网、车联网等新兴领域的快速发展，网络安全技术的应用场景不断拓展，市场需求持续增长。

技术类型	应用场景	国内主要研究机构 / 企业	技术进展
人工智能	入侵检测、威胁分析、安全决策	奇安信、360、清华大学	机器学习算法在攻击识别准确率提升至 95% 以上
大数据	安全审计、风险预警、态势感知	安恒信息、美亚柏科	支持 PB 级数据处理，分析效率提高 40%
区块链	数据存证、身份认证、供应链安全	蚂蚁集团、微众银行	在金融领域试点应用，交易安全性显著提升

量子通信加密	绝密信息传输、核心系统防护	中国科学技术大学、国盾量子	实现百公里级量子密钥分发
可信计算	终端安全、系统加固	联想、浪潮	构建可信计算环境，抵御恶意攻击能力增强

三、网络空间安全行业产业链分析

3.1 产业链结构概述

网络空间安全行业产业链涵盖了从上游的基础硬件与软件供应商，到中游的安全产品与服务提供商，再到下游的各类应用行业用户的完整生态体系。上游主要包括芯片、操作系统、数据库等基础软硬件供应商，为网络安全产品和服务提供底层支撑；中游是网络空间安全产业的核心，包括各类安全产品制造商和安全服务提供商，如防火墙、入侵检测系统、安全审计产品、安全咨询、安全运维等；下游则是广泛的应用行业，包括金融、能源、电信、政府、医疗、教育等各个领域，这些行业对网络安全有着不同程度的需求，是网络安全产品和服务的最终使用者。

3.2 产业链各环节分析

3.2.1 上游供应商

1.芯片：芯片是网络安全产品的核心组件之一，对产品的性能和安全性起着关键作用。在网络安全领域，专用安全芯片的需求日益增长，如用于加密解密、身份认证、安全存储等功能的芯片。国内一些企业在安全芯片研发方面取得了一定进展，如紫光国微、兆易创新等，但与国际先进水平相比，在芯片性能、集成度和功耗等方面仍存在差距。目前，部分高端安全芯片仍依赖进口，如英特尔的 SGX（Software Guard Extensions）芯片在可信计算领域应用广泛。

芯片类型	国内代表企业	产品特点	市场份额（国内）	国际竞争对手
加密芯片	紫光国微	支持多种加密算法，低功耗	25%	NXP、Microchip
身份认证芯片	兆易创新	高安全性、快速认证	20%	英飞凌、意法半导体
安全存储芯片	复旦微电子	防篡改、高可靠性	18%	三星、SK 海力士

2.操作系统：操作系统是网络安全的基础软件平台，其安全性直接影响到整个信息系统的安全。目前，全球主流操作系统主要由微软的 Windows、苹果的 macOS 和开源的 Linux 占据。在国内，国产操作系统如麒麟、统信 UOS 等在党政军等关键领域得到了一定的应用推广，但在市场份额和生态建设方面与国际主流操作系统仍有较大差距。操作系统的安全漏洞是网络攻击的重要目标，因此，操作系统厂商需要不断加强安全研发投入，及时修复安全漏洞，提高系统的安全性和稳定性。

操作系统类型	国内代表产品	应用领域	市场份额（国内）	国际竞争对手
桌面操作系统	统信 UOS	党政办公、教育	5%	Windows、macOS
	麒麟桌面操作系统	党政军、关键行业	6%	Windows、macOS
服务器操作系统	麒麟服务器操作系统	政务云、数据中心	8%	Windows Server、Linux
	统信服务器操作系统	企业级应用、云计算	7%	Windows Server、Linux

3.数据库：数据库存储着大量的关键业务数据，其安全性至关重要。主流数据库产品包括甲骨文的 Oracle、微软的 SQL Server、开源的 MySQL 等。国内数据库厂商如达梦、人大金仓等近年来发展迅速，在部分行业得到了应用。数据库安全主要涉及数据加密、访问控制、备份恢复等方面，随着数据安全法规的不断完善，对数据库安全的要求也越来越高。

数据库类型	国内代表产品	应用领域	市场份额（国内）	国际竞争对手
关系型数据库	达梦数据库	政务、金融、能源	12%	Oracle、SQL Server
	人大金仓数据库	党政、交通、电信	10%	Oracle、SQL Server
非关系型数据库	MongoDB（国产适配版）	互联网、大数据	8%	MongoDB（国际版）
	Redis（国产优化版）	缓存、实时计算	7%	Redis（国际版）

3.2.2 中游安全产品与服务提供商

安全产品

1.防火墙：防火墙是最基础的网络安全产品之一，用于在网络边界处阻挡外部非法网络访问和攻击。根据 Gartner 的数据，2024 年全球防火墙市场规模达到 80 亿美元，预计到 2029 年将增长至 120 亿美元。国内防火墙市场竞争激烈，以深信服、华为、奇安信等为代表的企业占据了较大市场份额。随着网络技术的发展，防火墙产品不断升级，从传统的包过滤防火墙向状态检测防火墙、应用层防火墙以及下一代防火墙（NGFW）演进，具备了更强大的应用识别、入侵防御和威胁检测能力。

企业名称	产品系列	核心功能	2024 年国内市场份额
深信服	AF 下一代防火墙	应用识别、入侵防御、智能运维	22%
华为	USG 系列防火墙	高性能防护、云管理、AI 威胁分析	20%
奇安信	NGFW 3600 系列	深度检测、联动防御、安全可视化	18%

2.入侵检测 / 防御系统（IDS/IPS）：IDS 用于实时监测网络流量，发现潜在的入侵行为并及时告警；IPS 则在 IDS 的基础上，能够自动对入侵行为进行阻断。2024 年全球 IDS/IPS 市场规模约为 50 亿美元，预计未来几年将保持稳定增长。国内 IDS/IPS 市场主要由启明星辰、绿盟科技等企业主导，产品在性能和功能上不断提升，能够检测和防御各类新型网络攻击，如 DDoS 攻击、零日漏洞攻击等。

企业名称	产品系列	检测能力	2024 年国内市场份额
启明星辰	天阗入侵检测系统	支持千万级流量检测，误报率低于 1%	25%
绿盟科技	NIPS 入侵防御系统	具备应用层威胁防护，可抵御 2000 + 种攻击	23%
安恒信息	明御入侵检测 / 防御系统	融合 AI 分析技术，检测准确率达 98%	15%

3.安全审计产品：安全审计产品用于对网络活动进行记录、分析和审查，帮助企业发现潜在的安全风险和违规行为。市场上的安全审计产品包括网络审计、主机审计、数据库审计等多种类型。随着企业对合规性要求的提高，安全审计产品的市场需

求不断增加。国内安全审计市场有安恒信息、美亚柏科等企业参与竞争，产品具备全面的审计功能和强大的数据分析能力，能够满足不同行业客户的需求。

企业名称	产品系列	审计功能	2024 年国内市场份额
安恒信息	明御运维审计与风险控制系统	支持网络、主机、数据库全场景审计，具备行为回溯功能	28%
美亚柏科	天眼电子数据取证分析系统	专注电子数据审计，可恢复删除数据并分析操作痕迹	22%
奇安信	奇安信日志审计系统	实现海量日志实时分析，支持多维度报表生成	18%

4.数据安全产品：随着数据安全法规的出台和企业对数据价值的重视，数据安全产品市场快速增长。数据安全产品主要包括数据加密、数据脱敏、数据防泄漏（DLP）等。2024 年全球数据安全产品市场规模达到 150 亿美元，预计到 2029 年将超过 300 亿美元。国内数据安全市场发展迅速，以亿赛通、明朝万达等为代表的企业在数据加密和 DLP 领域具有一定优势，产品能够有效保护企业的数据资产安全。

企业名称	产品系列	核心技术	2024 年国内市场份额
亿赛通	DataBackup 数据备份系统	采用先进的增量备份技术，备份效率提升 50%	26%
明朝万达	Chinasec（安元）数据安全平台	融合多模加密算法，支持数据全生命周期保护	23%
启明星辰	天玥数据安全审计系统	具备数据流向追踪，敏感数据识别准确率超 95%	17%

安全服务

1.安全咨询：安全咨询服务为企业提供网络安全战略规划、风险评估、合规咨询等专业服务。随着企业网络安全意识的提高和安全法规的不断完善，对安全咨询服务的需求日益增加。国际知名的安全咨询公司如埃森哲、毕马威等在全球市场占据领先

地位，国内也有一些专业的安全咨询机构，如赛可达实验室、中国信息安全测评中心等，为企业提供本地化的安全咨询服务。

企业 / 机构名称	服务领域	典型案例	2024 年国内市场份额
埃森哲	金融、电信等多行业安全战略规划	为某国有银行制定全面网络安全转型方案	18%
毕马威	合规咨询、风险评估	协助跨国企业完成 GDPR 合规改造	15%
赛可达实验室	网络安全产品评测、行业研究	发布年度网络安全产品白皮书	12%
中国信息安全测评中心	信息系统安全评估、认证	承担多个政务信息系统安全测评项目	10%

2.安全运维：安全运维服务负责企业网络安全系统的日常运行维护，确保安全设备的正常运行和安全策略的有效实施。安全运维服务包括安全设备巡检、漏洞修复、安全事件响应等内容。国内安全运维市场规模较大，许多网络安全企业都提供安全运维服务，如奇安信的安全运营中心（SOC）服务，能够为客户提供 7×24 小时的安全监测和应急响应服务，保障客户网络安全。

企业名称	服务模式	服务优势	2024 年国内市场份额
奇安信	安全运营中心（SOC）	AI 驱动的智能分析，响应时间缩短至分钟级	25%
深信服	一站式安全托管服务	全栈式安全产品与服务整合	20%
启明星辰	定制化运维服务	针对不同行业提供专属安全运维方案	18%

3.安全培训：安全培训服务旨在提高企业员工的网络安全意识和技能，减少人为因素导致的安全风险。安全培训内容包括网络安全基础知识、安全操作规范、应急处理方法等。市场上有许多专业的安全培训机构，如谷安天下、启明星辰安全学院等，通过线上线下相结合的方式，为企业和个人提供多样化的安全培训课程。

机构名称	培训方式	特色课程	2024 年国内市场份额

谷安天下	线上平台 + 线下实训	CISP（注册信息安全专业人员）认证培训	22%
启明星辰安全学院	企业定制化培训 + 公开课	网络安全攻防实战培训	18%
奇安信安全教育中心	VR 沉浸式教学	网络安全意识普及课程	15%

3.2.3 下游应用行业

1.金融行业：金融行业是网络安全的重点应用领域之一，涉及大量的客户资金和敏感信息。银行、证券、保险等金融机构对网络安全的要求极高，需要保障交易系统的安全稳定运行，防止客户信息泄露和金融诈骗。根据中国银行业协会的数据，2024 年我国银行业网络安全投入达到 500 亿元，占整个金融行业网络安全投入的 70% 以上。金融行业对网络安全产品和服务的需求涵盖了防火墙、入侵检测系统、数据加密、安全审计、身份认证等多个方面。

金融机构类型	主要安全需求	典型解决方案
银行	交易安全、客户信息保护、合规审计	部署下一代防火墙、数据加密系统、智能审计平台
证券	交易系统防护、防止恶意操纵、数据防泄漏	采用入侵防御系统、数字证书认证、DLP 解决方案
保险	保单数据安全、客户隐私保护、业务连续性	构建安全云平台、实施数据脱敏、建立灾备系统

2.能源行业：能源行业包括电力、石油、天然气等关键基础设施领域，其网络安全关系到国家能源安全和经济稳定。能源行业的生产控制系统通常采用工业控制系统（ICS），如 SCADA 系统、DCS 系统等，这些系统一旦遭受网络攻击，可能导致能源供应中断、生产事故等严重后果。近年来，能源行业加大了对网络安全的投入，加强了对工业控制系统的安全防护，如部署工业防火墙、工业入侵检测系统、安全隔离装置等安全产品。

能源子行业	安全风险点	防护措施
电力	电网调度系统攻击、电力监控系统入侵	部署电力专用防火墙、实施等保 2.0 三级防护

石油	油气管道控制系统破坏、数据篡改	采用工业级入侵检测系统、建立安全监测平台
天然气	储气库控制系统干扰、计量数据窃取	部署安全隔离装置、实现数据加密传输

3. 电信行业：电信行业作为网络基础设施的提供者，其网络安全直接影响到整个社会的通信服务质量。电信运营商需要保障通信网络的安全可靠运行，防止通信数据泄露和网络攻击。电信行业对网络安全的需求主要包括网络边界防护、核心网安全、数据中心安全、用户数据安全等方面。国内三大电信运营商中国移动、中国联通、中国电信在网络安全方面投入巨大，不断提升自身的安全防护能力，并与网络安全企业合作，共同应对网络安全挑战。

电信业务场景	安全需求	解决方案
移动通信网络	基站安全、用户身份认证	部署 5G 安全网关、采用生物识别技术
固定宽带网络	网络接入控制、流量监测	使用上网行为管理设备、搭建流量分析平台
数据中心	服务器安全、数据存储安全	实施服务器加固、采用分布式存储加密

4. 政府行业：政府部门掌握着大量的国家机密和公民个人信息，其网络安全至关重要。政府行业对网络安全的需求包括政务信息系统安全、电子政务网络安全、政府网站安全等方面。为了满足合规性要求和保障政务业务的正常开展，政府部门不断加大网络安全投入，采购各类网络安全产品和服务，如防火墙、入侵检测系统、安全审计产品、安全咨询服务等。同时，政府也积极推动网络安全产业的发展，通过政策引导和资金支持，鼓励企业加强技术创新和产品研发。

政府业务领域	安全重点	实施案例
电子政务	跨部门数据共享安全、政务云安全	某省政务云平台安全防护体系建设
公共服务	公民个人信息保护、在线服务系统安全	全国一体化政务服务平台安全加固
国家安全	涉密信息系统防护、网络情报分析	关键部门网络安全监测与响应平台搭建

5. **医疗行业**：医疗行业的数字化转型使得医疗信息系统面临着越来越多的网络安全风险，如患者病历信息泄露、医疗设备被攻击导致医疗事故等。因此，医疗行业对网络安全的需求日益增长，主要包括医院信息系统安全、医疗设备安全、患者数据安全等方面。医疗行业通常采购防火墙、数据加密产品、安全审计产品等网络安全产品，并加强员工的网络安全培训，提高整体的网络安全防护水平。

医疗场景	安全风险	应对措施
医院信息系统	电子病历泄露、医疗数据篡改	部署数据库审计系统、实施数据分级保护
医疗设备	手术机器人被控制、监护仪数据异常	采用设备准入控制、进行固件安全升级
远程医疗	通信数据泄露、身份假冒	使用加密通信协议、多因素认证技术

6. **教育行业**：随着在线教育的快速发展和教育信息化的深入推进，教育行业的网络安全问题也逐渐凸显。学校需要保障校园网络的安全，防止学生信息泄露和教学资源被盗用。教育行业对网络安全的需求主要包括校园网络边界防护、教育信息系统安全、在线教育平台安全等方面。学校通常会采购防火墙、入侵检测系统、上网行为管理设备等网络安全产品，并加强对师生的网络安全宣传教育，提高网络安全意识。

教育场景	安全需求	实现方式
校园网络	学生上网行为管理、防止恶意攻击	部署上网行为管理设备、配置防火墙策略
教育信息系统	学籍数据保护、选课系统安全	实施数据加密、进行定期安全漏洞扫描
在线教育平台	课程资源防盗版、用户身份验证	采用数字水印技术、双因素认证机制

3.3 产业链上下游关系及影响

产业链上下游之间存在着紧密的依存关系。上游基础硬件与软件供应商为中游安全产品与服务提供商提供技术和产品支持，其技术水平和产品质量直接影响到中游企业的产品性能和安全性。例如，高性能的安全芯片能够提升防火墙、加密设备等安全产品的处理能力和加密强度；稳定可靠的操作系统和数据库为安全产品的运行提供良好的软件环境。同时，中游企业的市场需求也会反馈到上游供应商，促使其不断进行技术创新和产品升级，以满足网络安全行业日益增长的需求。

中游安全产品与服务提供商则是连接上下游的关键环节，其产品和服务直接面向下游应用行业用户。中游企业通过不断研发创新，提供满足不同行业需求的网络安全解决方案，推动了网络安全技术在各个行业的应用和普及。下游应用行业用户的需求是产业链发展的主要驱动力，不同行业对网络安全的需求特点和侧重点不同，促使中游企业不断优化产品和服务，提高行业针对性和解决方案的有效性。同时，下游行业的发展状况和投入水平也直接影响到中游企业的市场规模和盈利能力。

上下游之间的协同合作对于网络空间安全行业的发展至关重要。通过加强产业链上下游之间的沟通与协作，建立良好的生态合作关系，能够实现资源共享、优势互补，共同应对日益复杂的网络安全威胁，推动网络空间安全产业的健康、快速发展。例如，上游供应商与中游企业可以联合开展技术研发，共同攻克关键技术难题；中游企业与下游行业用户可以深入合作，了解行业实际需求，开发出更贴合用户需求的产品和服务。

四、网络空间安全行业市场需求分析

4.1 不同行业的网络空间安全需求特点

4.1.1 金融行业

1.高安全性要求：金融行业涉及海量资金交易和客户敏感信息，如银行卡号、密码、身份证号等，一旦发生安全事故，将导致严重的经济损失和客户信任危机。因此，金融行业对网络安全的安全性要求极高，需要确保交易系统的绝对安全，防止黑客攻击、数据泄露和金融诈骗等风险。

2.严格的合规性需求：金融行业受到严格的监管，各国都制定了一系列法律法规和监管标准，如巴塞尔协议、PCI - DSS（支付卡行业数据安全标准）等。金融机构必须满足这些合规要求，通过定期的安全审计和评估，确保网络安全体系符合相关标准，否则将面临巨额罚款和业务限制。

3.实时性与连续性需求：金融交易具有实时性特点，要求网络安全系统能够实时监测和防御攻击，确保交易的连续性。任何短暂的系统中断或服务故障都可能导致巨大的经济损失，因此金融机构需要具备高可用性的网络安全解决方案，包括灾备系统、业务连续性计划等。

4.1.2 医疗行业

1.患者数据安全优先：医疗行业存储着大量患者的敏感信息，包括病历、诊断结果、治疗记录等，这些数据的泄露可能导致患者隐私泄露、身份被盗用等问题，甚至影响患者的生命安全。因此，保护患者数据安全是医疗行业网络安全的首要任务，需要采用严格的数据加密、访问控制和审计措施。

2. 医疗设备安全关键：随着医疗设备的智能化和联网化，医疗设备面临着被攻击的风险，如手术机器人被控制、输液泵参数被篡改等，可能直接威胁患者的生命健康。因此，医疗设备的安全防护至关重要，需要确保设备的固件安全、通信安全和操作安全。

3. 业务连续性需求：医疗服务的连续性直接关系到患者的救治效果，网络安全事件导致的医疗系统中断可能延误患者的治疗。因此，医疗行业需要具备可靠的灾备和应急响应机制，确保在遭受网络攻击或系统故障时，能够快速恢复业务运行。

4.1.3 政府行业

1. 国家机密保护：政府部门掌握着大量涉及国家安全、政治稳定的机密信息，这些信息一旦泄露，将对国家利益造成严重损害。因此，政府行业对网络安全的保密性要求极高，需要采用高强度的加密技术、严格的访问控制和安全审计措施，确保机密信息的安全。

2. 合规性与公信力需求：政府部门需要遵守国家相关法律法规和政策要求，确保网络安全体系符合国家信息安全等级保护制度等标准。同时，政府网络安全的可靠性和稳定性直接影响政府的公信力，任何安全事件都可能引发公众的质疑和不满，因此政府需要建立完善的网络安全防护体系和应急响应机制。

3. 跨部门协同安全需求：随着电子政务的发展，政府部门之间的信息共享和业务协同日益频繁，这就要求建立统一的网络安全框架，实现跨部门的安全协同防护，确保信息在共享和传输过程中的安全。

4.1.4 能源行业

1. 关键基础设施安全：能源行业的生产控制系统是国家关键信息基础设施的重要组成部分，其安全运行关系到国家能源安全和社会稳定。一旦遭受网络攻击，可能导致能源供应中断、生产事故等严重后果，因此能源行业对网络安全的可靠性和稳定性要求极高，需要采用工业级的安全防护设备和技术。

2. 长周期与高风险特点：能源行业的生产设施建设和运行周期长，网络安全风险贯穿整个生命周期。同时，能源生产过程中的安全事故往往会造成巨大的经济损失和环境破坏，因此能源企业需要建立长期的网络安全规划和风险管理体系，持续监测和防范安全风险。

3. 工业控制系统安全：能源行业广泛采用工业控制系统，这些系统具有专业性强、实时性高、协议封闭等特点，传统的网络安全技术难以有效防护。因此，能源行业需要针对工业控制系统的特点，开发专用的安全防护产品和解决方案，确保工业控制系统的安全运行。

4.2 网络空间安全攻击事件典型案例分析

4.2.1 金融行业案例 - Depot 勒索软件攻击

2024 年 1 月 8 日，美国最大的零售抵押贷款机构之一 LoanDepot 遭受了一场严重的勒索软件攻击。攻击者成功入侵其系统，致使部分关键业务系统被迫下线。此次攻击造成了约 1660 万客户的敏感个人信息被盗取，其中涵盖社会保障号码以及金融账户号码等极为重要的数据。LoanDepot 为应对此次危机，花费了高达 2690 万美元的资金，用于补救受损系统、通知受影响客户以及支付相关法律费用等方面。这一事件充分暴露了金融行业在面对勒索软件攻击时的脆弱性，大量客户敏感信息的泄露不仅可能导致客户遭遇经济损失，如身份被盗用进行金融诈骗等，还对 LoanDepot 的企业声誉造成了极大的负面影响，客户信任度大幅下降，在市场竞争中面临严峻挑战。同时，该事件也反映出金融机构在网络安全防护体系上可能存在漏洞，未能有效抵御此类针对性强的勒索软件攻击，在数据备份、应急响应以及安全监测等方面需要进一步加强。

4.2.2 医疗行业案例 - Change Healthcare 勒索软件攻击

2024 年 2 月，美国医疗支付提供商 Change Healthcare 遭遇勒索软件攻击，此次攻击导致全国范围内患者处方及其他医疗服务出现严重延误。攻击者加密了大量关键医疗数据，使得医疗机构无法正常调取患者信息，影响了诊断和治疗流程。为恢复系统运行，Change Healthcare 的母公司 UnitedHealth Group 支付了 2200 万美元赎金。更严重的是，该事件导致约 1 亿条个人医疗数据泄露，成为美国医疗行业史上规模较大的数据泄露事件之一。这不仅侵犯了患者隐私权，还可能因医疗数据错误或缺失对患者生命健康造成威胁。此案例表明，医疗行业数字化进程中，医疗信息系统和设备的安全防护亟待加强，同时也凸显了建立完善的数据备份和应急恢复机制的重要性。

4.2.3 政府行业案例 - 美国对中国某先进材料设计研究单位网络攻击

自 2024 年 8 月起，国家互联网应急中心监测发现，美国疑似针对我国某先进材料设计研究单位发动网络攻击，企图窃取商业秘密信息。攻击者利用我国境内某电子文档安全管理系统存在的漏洞，入侵该公司部署的软件升级管理服务器，通过软件升级服务向 270 余台主机植入控制木马。这些木马允许攻击者远程操控主机，进而窃取大量商业秘密和知识产权。此次攻击属于典型的网络间谍行为，严重威胁我国关键领域的技术安全和创新发展。这警示政府相关部门和科研机构，需强化网络安全防护体系，提高对系统漏洞的监测和修复能力，加强核心数据的保护措施，防范境外势力的网络窃密活动。

4.2.4 能源行业案例 - 西北能源基地 DNS 篡改事件

2025 年 1 月，某境外组织对我国西北能源基地实施网络攻击，试图通过篡改路由器的 DNS 设置阻断数据传输，意图引发区域性停电事故。攻击者采用供应链攻击手

段，先入侵能源企业供应商系统并植入恶意代码，再篡改 DNS 配置，同时利用加密隧道与境外 C2 服务器通信以躲避检测。甘肃网警迅速响应，72 小时内锁定攻击源并实施反制，成功恢复系统运行。事件发生后，我国加强能源行业网络安全防护，建立“芯片 - 操作系统 - 应用软件” 全链条安全审查机制，华为、奇安信等企业推出“攻击面管理平台”，实现网络资产动态测绘和风险闭环管理。该案例凸显能源行业网络安全对国家能源供应和社会稳定的重要性，也体现了应对新型网络攻击需要产业链协同防护和技术创新。

4.2.5 教育行业案例 - 多所高校遭受勒索软件攻击

2024 年 12 月，我国清华大学、北京大学等多所高校成为勒索软件攻击目标。攻击者通过伪造学术会议邀请函的钓鱼邮件，诱导研究人员点击恶意链接，进而在高校内网植入恶意软件。利用内网漏洞，恶意软件横向渗透至核心服务器，加密大量科研数据并索要比特币赎金。教育部迅速启动 “护网行动”，排查出高校网络安全漏洞 3.2 万个，处置攻击 1.8 亿次。安恒信息的 AI 安全检测平台对 Deepfake 等新型攻击识别准确率达 99.7%，发挥重要作用。事件发生后，高校加强师生网络安全培训，建立 “学术数据安全沙箱” 保护科研数据，同时推动《生成式 AI 安全评估规范》发布，加强教育领域 AI 应用的安全监管。

五、网络空间安全行业人才需求分析

5.1 人才需求现状

随着网络空间安全行业的快速发展，市场对专业人才的需求呈现爆发式增长。根据《中国网络安全人才发展报告》显示，2024 年我国网络安全人才缺口已达 140 万人，且预计在未来几年内，这一缺口将持续扩大。各行业对网络安全人才的需求涵盖了技术研发、安全运维、安全分析、安全管理等多个领域。在技术研发方面，需要具备扎实的编程基础和网络安全知识的人才，以开发新型安全产品和解决方案；安全运维人员则负责保障企业网络安全系统的日常运行和维护；安全分析人才专注于对网络安全事件和数据进行深入分析，及时发现潜在威胁；安全管理人员则从战略层面规划和管理企业的网络安全体系。

人才类型	主要职责	企业需求占比
技术研发人才	开发防火墙、入侵检测系统等安全产品	35%
安全运维人才	保障网络安全系统日常运行和维护	30%

安全分析人才	分析网络安全事件和数据，发现潜在威胁	20%
安全管理人才	规划和管理企业网络安全体系	15%

5.2 人才培养现状

目前，我国网络空间安全人才培养主要通过高校教育、职业培训和企业内部培训三种途径。在高校教育方面，越来越多的高校开设了网络空间安全相关专业，如网络安全、信息安全等，课程设置涵盖了网络原理、密码学、网络攻击与防御、数据安全等核心内容。然而，高校教育在实践教学环节相对薄弱，培养的人才与企业实际需求存在一定差距。职业培训机构则侧重于培养学生的实践技能，通过模拟真实的网络安全场景，让学生掌握实际操作能力，但在理论知识的系统性和深度上有所欠缺。企业内部培训主要针对在职员工，帮助他们提升专业技能和更新知识，但难以满足企业对大量新增人才的需求。

培养途径	优势	不足
高校教育	理论知识系统全面	实践教学薄弱，与企业需求脱节
职业培训	注重实践技能培养	理论知识不够系统深入
企业内部培训	贴合企业实际需求	难以满足大量新增人才需求

5.3 人才供需矛盾及原因

当前，网络空间安全行业人才供需矛盾突出。一方面，行业快速发展带来大量人才需求；另一方面，人才培养体系难以在短时间内培养出足够数量且符合企业需求的专业人才。造成这一矛盾的原因主要有以下几点：首先，网络空间安全是一个新兴且技术更新迅速的领域，高校教育的课程体系和教学方法更新速度较慢，难以跟上技术发展的步伐。其次，网络安全人才培养需要大量的实践教学资源和专业师资，但目前很多高校和培训机构在这方面存在不足。此外，网络安全行业对人才的综合素质要求较高，不仅需要掌握专业技术知识，还需要具备良好的沟通能力、团队协作能力和应急处理能力，这也增加了人才培养的难度。

六、网络空间安全行业技术发展趋势

6.1 人工智能与机器学习的深度应用

未来，人工智能与机器学习将在网络空间安全领域得到更深入的应用。通过对海量网络安全数据的学习和分析，AI 算法能够更精准地识别网络攻击模式，实现对未知威胁的提前预警。例如，利用深度学习算法构建的入侵检测模型，可以自动学习正常网络行为的特征，当出现异常行为时及时发出警报。同时，AI 技术还可以应用于安全运维领域，实现安全设备的自动化管理和策略优化，提高运维效率，减少人为错误。

6.2 零信任架构的普及

零信任架构以 “永不信任，始终验证” 为原则，打破了传统网络安全中基于网络位置的信任模式。在零信任架构下，无论用户或设备位于网络内部还是外部，都需要经过严格的身份认证和权限验证才能访问资源。随着网络边界的日益模糊，零信任架构将逐渐成为企业网络安全防护的主流模式，有效降低内部攻击和数据泄露的风险。

6.3 物联网与工业互联网安全技术升级

随着物联网和工业互联网设备数量的爆发式增长，其安全问题日益突出。未来，针对物联网和工业互联网的安全技术将不断升级，包括设备身份认证、通信加密、漏洞检测等方面。例如，采用轻量级加密算法保障物联网设备在资源受限情况下的通信安全，开发专门的工业互联网安全监测平台，实时监控工业控制系统的安全状态。

6.4 量子通信与加密技术的突破

量子通信和加密技术具有理论上绝对安全的特性，将为网络空间安全带来革命性变化。目前，我国在量子通信领域已取得一定成果，实现了百公里级量子密钥分发。未来，随着量子通信技术的进一步突破和商业化应用，将为金融、政务等对安全性要求极高的领域提供更可靠的通信和数据加密解决方案。

七、网络空间安全行业未来发展挑战与机遇

7.1发展挑战

1.技术创新压力：网络攻击技术不断演进，如高级持续性威胁（APT）、深度伪造（Deepfake）等新型攻击手段层出不穷，对网络安全技术创新提出了更高要求。企业和研究机构需要持续投入大量资源进行技术研发，以应对不断变化的安全威胁，这对企业的资金和技术实力都是巨大挑战。

2.人才短缺制约：如前文所述，网络空间安全行业人才缺口巨大，人才短缺严重制约了行业的发展速度和创新能力。企业难以招聘到足够数量和质量的专业人才，导致项目推进缓慢，安全防护水平提升困难。

3.国际竞争加剧：在全球网络空间安全市场中，我国企业面临着来自国际巨头的激烈竞争。国际企业在技术研发、品牌影响力和市场份额等方面具有优势，我国网络安全企业需要在国际市场中不断提升自身竞争力，突破技术壁垒，拓展海外市场。

7.2发展机遇

1．政策支持力度加大：我国政府高度重视网络空间安全，未来将继续出台一系列政策法规支持行业发展，加大对网络安全产业的资金投入和政策扶持。这将为企业提供良好的发展环境，促进产业集聚和技术创新。

2.数字化转型加速需求：随着各行业数字化转型的加速，对网络安全的需求将持续增长。云计算、大数据、物联网等新兴技术的广泛应用，将创造更多的网络安全应用场景，为网络安全企业带来广阔的市场空间。

3.技术融合带来创新机遇：人工智能、区块链、量子技术等新兴技术与网络安全的融合，将催生新的安全技术和解决方案。企业可以抓住技术融合的机遇，开展创新研发，推出具有竞争力的新产品和服务，开辟新的市场领域。

八、结论

网络空间安全行业作为保障国家安全和经济社会发展的重要产业，在数字化时代具有广阔的发展前景。当前，全球和我国网络空间安全市场规模持续增长，技术创新不断推进，应用领域日益拓展，但同时也面临着技术创新压力大、人才短缺、国际竞争加剧等挑战。未来，随着政策支持的加强、数字化转型的加速以及技术融合的深入，网络空间安全行业将迎来新的发展机遇。高校在申报网络空间安全专业时，应充分考虑行业发展需求，优化专业课程设置，加强实践教学，培养适应市场需求的高素质专业人才，为我国网络空间安全产业的发展提供有力的人才支撑。

5. 申请增设专业人才培养方案

网络空间安全专业人才培养方案

一、专业代码

专业名称：网络空间安全

专业代码：080911TK

总 学 分：160

二、专业介绍

网络空间安全是保障个人权益、社会稳定、国家主权与全球数字经济健康发展的核心基石，本专业专业聚焦数字文化产业安全，依托学校在数字文旅、人工智能设计、数字修复和版权保护方面的多年积累。围绕数字艺术内容安全、艺术装备安全、AIGC 艺术伦理与安全治理等特色方向，深化“校企合作、产学结合”实践模式，以数字艺术内容安全等产业需求为切入点，注重为学生构筑扎实理论基础和专业知识体系，强化学生在网络空间安全应用领域的实践能力和创新意识，为辽宁省乃至东北的网络空间安全战略和数字文化安全产业培养高素质应用型人才。

三、培养目标

本专业立足大连，面向东北，服务区域数字文化产业网络空间安全，培养德智体美劳全面发展，掌握网络空间安全、计算机科学与技术基本理论和知识，具备网络安全系统开发、安全算法设计、安全风险评估、网络攻防实战以及艺术类数字内容与设备安全保障等研发能力，能够在网络空间安全及相关领域，如政府部门、金融机构、互联网企业、艺术与创意产业等，从事网络安全防护、信息系统安全架构设计、数据安全管理、安全产品研发、数字艺术内容保护以及智能设备安全管理等相关工作的高素质应用型人才。

本专业学生在毕业后 5 年能够达到以下目标：

目标 1：掌握从事信息安全领域所需的数学、信息安全基础、计算机科学与技术基本理论和知识。

目标 2：具备分析、解决信息安全领域实际工程问题的能力，具备在艺术作品保护、数字版权管理等领域相关产品的设计、研发及测试等工作中合理运用现代工具和新技术成果开展创新型应用的能力。

目标 3：了解网络空间安全的发展现状和趋势，能够在数字艺术创作安全审核中平衡创新表达与内容合规，制定兼顾文化传播需求与数据安全保护的解决方案，能够坚守文化安全红线，在艺术内容应用场景中维护国家文化安全。

目标 4：熟悉网络空间安全及其交叉学科领域相关的工程管理基本原理与经济决策方法，能够进行良好的表达、沟通与团队协作合作，胜任研发、测试、技术支持等部门的管理工作。

目标 5：具备良好的文化素养和较强的社会责任感、较好的信息安全领域职业道德和职业素养。

四、毕业要求

通过专业学习，毕业生应获得以下几方面的知识、能力和素质：

0.思想品德

具有坚定正确的政治方向，热爱祖国，热爱人民，拥护中国共产党的领导；具有正确的世界观、人生观、价值观，具有良好的思想品德、健全的人格、健康的体魄，践行社会主义核心价值观。

0.1 具有坚定正确的政治方向，热爱祖国，热爱人民，拥护中国共产党的领导，具有正确的世界观、人生观、价值观；

0.2 具有良好的思想品德、健全的人格、健康的体魄，践行社会主义核心价值观；

0.3 具有良好的人文素养、科学素养、数字素养、艺术修养、审美能力和劳动素养。

1.工程知识

掌握本专业所需的数学、自然科学、工程基础和专业知识，并能够用于解决网络空间安全领域的复杂工程问题。

1.1 掌握数学及自然科学的基本概念和理论，能够将数学建模、推理等方法，运用于网络空间安全领域复杂工程问题的设计与分析；

1.2 掌握网络空间安全领域的工程基础知识，能够运用数字电子技术和计算机系统基础原理，分析网络空间安全领域的复杂工程问题；

1.3 掌握网络空间安全基础理论，能够用于对网络空间安全领域复杂工程问题的设计方案或模型进行推理和验证；

1.4 能够运用专业知识，对网络空间安全领域复杂工程问题的解决方案进行分析、改进。

2.问题分析

能够应用数学、自然科学和工程科学的基本原理，识别、表达并通过文献研究分析网络空间安全领域中遇到的复杂工程问题，以获得有效结论。

2.1 能够运用数理知识和工程科学基本原理，识别和判断网络空间安全领域复杂工程问题中的关键环节和参数；

2.2 能够运用数理知识和工程科学基本原理，假设和简化复杂的网络空间安全应用系统和环境，并基于网络空间安全专业知识，通过建模等方法，制定和表达网络空间安全领域复杂工程问题的解决方案、思路和方法；

2.3 能够理解网络空间安全领域复杂工程问题有多种解决方案可选择，并能够运用文献研究、实验、经验提炼等方法，寻求可替代的解决方案；

2.4 能够基于网络空间安全领域复杂工程问题解决过程中的技术、社会等影响因素，

分析和判断解决方案的合理性与可行性，以获得有效结论。

3.设计/开发解决方案

能够针对网络空间安全领域的复杂工程问题设计和开发解决方案，设计满足特定需求的系统、单元（部件）或工艺流程，能够在设计环节中体现创新意识，并从健康、安全与环境、法律、社会与文化等角度考虑可行性。

3.1 掌握专业领域的基本设计方法和开发技术，了解影响设计目标和技术方案的各种因素；

3.2 能够针对具体的功能性需求和性能约束，确定系统、模块或安全策略。能够结合网络空间应用场景的约束，设计切实可行的解决方案，并在设计中体现创新意识；

3.3 理解影响设计目标和技术方案的技术因素和非技术因素，能在解决方案中考虑安全、健康、法律、文化及环境等制约因素；

3.4 能够对解决方案进行测试和评价，用图表、设计报告、软硬件等形式呈现设计成果。

4.研究

能够基于科学原理并采用科学方法对网络空间安全领域的复杂工程问题进行研究，包括设计实验、分析与解释数据，并通过信息综合得到合理有效的结论。

4.1 能够运用科学方法，对网络空间安全领域的复杂工程问题进行需求和功能分析；

4.2 能够基于网络空间安全基础理论，针对问题选择研究路线，设计实验方案；

4.3 能够根据实验方案选用或搭建合适的平台，设计原型系统或者仿真实验；

4.4 能够正确采集、整理实验数据，对实验结果进行分析和解释，获取合理有效的结论。

5.使用现代工具

能够针对网络空间安全领域的复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，包括对网络空间安全领域复杂工程问题的预测与模拟，并能够理解其局限性。

5.1 具备信息技术应用能力，熟悉常用的 AI 工具和应用平台；

5.2 能够根据网络空间安全领域复杂工程问题的设计需要，开发、选择与使用恰当的平台、技术、资源和现代工程工具；

5.3 能够对网络空间安全领域复杂工程问题进行预测、模拟、设计及实现的优势与局限性。

6.工程与可持续发展

能够基于网络空间安全专业相关背景知识进行合理分析，评价网络空间安全专业实践和复杂工程问题解决方案，对健康、安全、环境、法律以及经济和社会可持续发展的影响，并理解应承担的责任。

6.1 具有网络空间安全领域的工程实习和社会实践经历，了解与网络空间安全行业相关的技术标准、知识产权、产业政策和法律法规；

6.2 能够通过合理分析，对网络空间安全领域的新系统、新技术的开发和应用、相关复杂工程问题的解决方案等对社会、健康、安全、法律以及文化的潜在影响进行评价，并理解应承担的责任；

6.3 能够理解环境保护和社会可持续发展的内涵和意义，了解环境保护的相关法律法规；

6.4 能够理解和评价网络空间安全工程实践的资源利用效率、安全防范措施等对环境和社会可持续 发展的影响。

7.工程伦理和职业规范

有工程报国、为民造福的意识，具有人文社会科学素养和社会责任感，能够在网络空间安全领域复杂工程问题的工程实践中理解和践行工程伦理，遵守工程职业道德、规范和相关法律，履行责任。

7.1 具有健康的身心，能够诚信守则，关爱他人，具有人文知识、思辨能力和科学精神；

7.2 树立正确的世界观、人生观、价值观，了解国情，维护国家利益，具有推动民族复兴和社会进 步的责任感；

7.3 能够理解网络空间安全工程师的职业性质、职业道德和责任，能够在工程实践中自觉遵守职业规范，具有法律意识；

8.个人与团队

能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色。具有较强的协作、组织和管理能力。

8.1 能够正确认识自我，具有团队意识，主动与其他学科的成员共享信息，合作共事；

8.2 能够理解团队中每个角色的含义及在团队中的作用，能够在多学科背景下的团队中胜任自己所承担的个体、团队成员以及负责人等各种角色；

8.3 能够与团队的成员进行有效沟通，能够实施团队工作的过程管理。

9.沟通

能够就网络空间安全领域复杂工程问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令，并具备一定的国际视野，能够在跨文化背景下进行沟通和交流。

9.1 具有良好的语言表达和文字组织能力，能够通过口头、文稿、图表等方式清晰准确地表达网络空间安全领域的相关问题，与专业人士及社会公众进行有效沟通和交流，

能够遵循学术规范完成毕业论文撰写，包括研究问题界定、研究框架搭建、实证分析或实践论证；

9.2 具有一定的外语听、说、读、写能力，了解本行业的国际现状和发展趋势，能够在跨文化背景下进行沟通和交流；

9.3 能够查阅网络空间安全领域的国外技术文献，能够以良好的国际视野在跨文化背景下进行沟通和交流。

10.项目管理

理解并掌握网络空间安全行业所涉及的工程管理原理与经济决策方法，并能够在多学科环境中应用。

10.1 掌握工程项目管理的知识和技能，具备理论与实践结合的项目管理能力；

10.2 能够将工程管理和经济学的基本原理应用于多学科交叉的工程实践中，优化系统项目的设计、开发和实施。

11.终身学习

具有自主学习和终身学习的意识，具有不断学习和适应社会发展的能力。

11.1 能够理解个人成长与职业发展需求的关系，认识不断探索和学习的必要性，具有自主学习和终身学习的意识；

11.2 了解拓展知识和能力的途径，能够通过自主学习，解决在网络空间安全领域复杂工程问题的设计及实现中的问题。

五、“培养目标-毕业要求”和“毕业要求-课程设置”对应矩阵

（一）“培养目标-毕业要求”对应矩阵

培养目标 毕业要求	目标 1	目标 2	目标 3	目标 4	目标 5
毕业要求 1	●	●			
毕业要求 2	●	●			
毕业要求 3	●	●			
毕业要求 4	●	●			
毕业要求 5	●	●			●
毕业要求 6	●		●		
毕业要求 7			●		
毕业要求 8			●		
毕业要求 9				●	
毕业要求 10				●	●
毕业要求 11				●	

“毕业要求—课程体系”对应矩阵

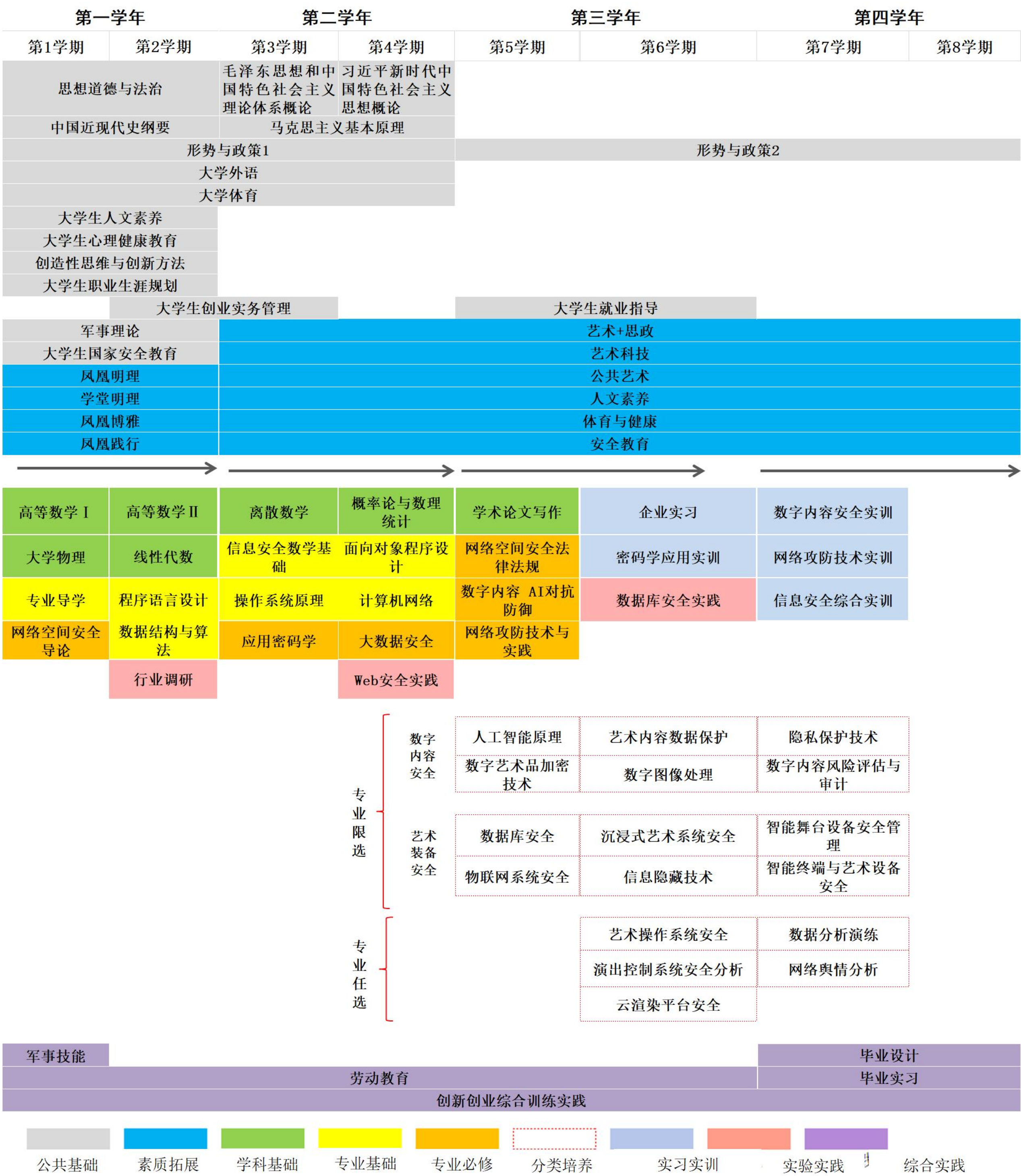
课程名称	毕业要求																																					
	0 思想品德			1 工程知识				2 问题分析				3 设计/开发解决方案				4 研究				5 使用现代工具			6 工程与可持续发展				7 工程伦理和职业规范			8 个人与团队			9 沟通			10 项目管理		11 终身学习	
	0.1	0.2	0.3	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4	5.1	5.2	5.3	6.1	6.2	6.3	6.4	7.1	7.2	7.3	8.1	8.2	8.3	9.1	9.2	9.3	10.1	10.2	11.1	11.2
思想道德与法治	M	H																												L									
中国近现代史纲要	H	M																												L									
马克思主义基本原理	H		M																											L									
毛泽东思想和中国特色社会主义理论体系概论	H		M																											L									
习近平新时代中国特色社会主义思想概论	H	M																												L									
大学生国家安全教育	H	L																												M									
形势与政策	H	M																												L									
大学外语			L																														M	H					
大学体育	L	H																												M									
大学生人文素养	L		M																								M						H						
军事理论	H	L																												M									
军事技能	H	L																												M									
大学生职业生涯规划	H																													M			L						
大学生心理健康教育		H	L																														M						
大学生就业指导	H																													M			L						
大学生创业实务管理	M																														L					H			
创造性思维与创新方法	H																			M												L							
劳动教育	M		H																											L									
高等数学Ⅰ				H				H								M																							

课程名称	毕业要求																																						
	0 思想品德			1 工程知识				2 问题分析				3 设计/开发解决方案				4 研究				5 使用现代工具			6 工程与可持续发展				7 工程伦理和职业规范			8 个人与团队			9 沟通			10 项目管理		11 终身学习	
	0.1	0.2	0.3	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4	5.1	5.2	5.3	6.1	6.2	6.3	6.4	7.1	7.2	7.3	8.1	8.2	8.3	9.1	9.2	9.3	10.1	10.2	11.1	11.2
大学物理			L	H				M																															
高等数学Ⅱ				H				M														L																	
线性代数				H															M							L													
离散数学						H			M																														
概率论与数理统计				H																						M									L				
学术论文写作										M																							H						L
程序语言设计												H								M							L												
数据结构与算法							H						M																								L		
操作系统原理					H																		M									L							
信息安全数学基础						H							M														L												
数据库系统原理及应用			L																				H									M							
面向对象程序设计												H									M												L						
计算机网络					H									M										L															
网络空间安全导论			H																									M										L	
应用密码学						H							M																L										
大数据安全																								H								M					L		
网络空间安全法律法规	L																						H						M										
数字内容 AI 对抗防御												H								M														L					
网络攻防技术与实践															H			M																		L			
人工智能原理													L							M													L						
数字艺术品加密与确权			L										M																	L									
艺术内容数据安全防护与溯源																					L				M		L												
数字图像处理			L									M									L																		

课程名称	毕业要求																																						
	0 思想品德			1 工程知识				2 问题分析				3 设计/开发解决方案				4 研究				5 使用现代工具			6 工程与可持续发展				7 工程伦理和职业规范			8 个人与团队			9 沟通			10 项目管理		11 终身学习	
	0.1	0.2	0.3	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4	5.1	5.2	5.3	6.1	6.2	6.3	6.4	7.1	7.2	7.3	8.1	8.2	8.3	9.1	9.2	9.3	10.1	10.2	11.1	11.2
隐私保护技术																								M					L				L						
数字内容风险评估与审计											L															M										L			
数据库安全														L									M									L							
物联网系统安全														M							L			L															
沉浸式艺术系统安全																		M			L																L		
信息隐藏技术													M																L				L						
智能舞台设备安全管理																								M							L					L			
智能终端与艺术设备安全														M																L									
艺术操作系统安全			L		M																		L																
演出控制系统安全分析																								M													L		
云渲染平台安全														M							L																		
数据分析演练											L								M																				
网络舆情分析																								M												L			
行业调研										M																							L						
Web 安全实践															M			L																					
数据库安全实践																		M				L										L							
企业实习																							M																M
密码学应用实训																			M										L										
数字内容安全实训															M															L									
网络攻防技术实训														M				L																					
信息安全综合实训															M																					L			
毕业设计																																	M					L	
毕业实习																							M														L		

注：H 为高支撑，M 为中支撑，L 为低支撑

六、课程体系拓扑图



第一学年
第二学年
第三学年
第四学年
第1学期
第2学期
第3学期
第4学期
第5学期
第6学期
第7学期
第8学期
思想道德与法治
毛泽东思想和中国特色社会主义理论体系概论
习近平新时代中国特色社会主义思想概论
中国近现代史纲要
马克思主义基本原理
形势与政策1
形势与政策2
大学外语
大学体育
大学生人文素养
大学生心理健康教育
创造性思维与创新方法
大学生职业生涯规划
大学生创业实务管理
大学生就业指导
军事理论
艺术+思政
大学生国家安全教育
艺术科技
凤凰明理
公共艺术
学堂明理
人文素养
凤凰博雅
体育与健康
凤凰践行
安全教育
高等数学Ⅰ
高等数学Ⅱ
离散数学
概率论与数理统计
学术论文写作
企业实习
数字内容安全实训
大学物理
线性代数
信息安全数学基础
面向对象程序设计
网络空间安全法律法规
密码学应用实训
网络攻防技术实训
专业导学
程序语言设计
操作系统原理
计算机网络
数字内容 AI对抗防御
数据库安全实践
信息安全综合实训
网络空间安全导论
数据结构与算法
应用密码学
大数据安全
网络攻防技术与实践
行业调研
Web安全实践
专业限选
数字内容安全
人工智能原理
艺术内容数据保护
隐私保护技术
数字艺术品加密技术
数字图像处理
数字内容风险评估与审计
艺术装备安全
数据库安全
沉浸式艺术系统安全
智能舞台设备安全管理
物联网系统安全
信息隐藏技术
智能终端与艺术设备安全
专业任选
艺术操作系统安全
数据分析演练
演出控制系统安全分析
网络舆情分析
云渲染平台安全
军事技能
毕业设计
劳动教育
毕业实习
创新创业综合训练实践
公共基础
素质拓展
学科基础
专业基础
专业必修
分类培养
实习实训
实验实践
综合实践

七、主干学科、核心课程、特色课程

主干学科：网络空间安全、计算机科学与技术

核心课程： 网络空间安全导论、应用密码学、大数据安全、网络空间安全法律法规、数字内容 AI 对抗防御、网络攻防技术与实践

特色课程：数字艺术品加密技术、艺术元数据保护、智能终端与艺术设备安全、智能舞台设备安全运维与管理、沉浸艺术安全风险综合实验、艺术操作系统安全

八、主要实践性教学各环节

主要实验与实训：企业实训、密码学应用实训、数字内容安全实训、网络攻防技术实训、信息安全综合实训

主要实践性教学环节：认知实习、专业实习、毕业实习、毕业设计

九、修业年限、学分要求和学位授予

修业年限：4 年，学生可在 4-6 年内修完本专业规定学分。

学分要求：本专业学生在学习期间必须修满培养方案规定的 160 学分方能毕业。

授予学位：修满规定学分，符合《中华人民共和国学位条例》及《大连艺术学院本科毕业生学士学位授予办法》，授予工学学士学位。

十、课程体系设计

（一）课程体系总体设计

<table>
<tr><th>课程平台</th><th colspan="4">课程类别</th><th>课程性质</th><th>学分/实践学分</th><th>学时</th><th>实践学分占总学分比例</th></tr>
<tr><td rowspan="2">通识教育</td><td rowspan="8">第一课堂</td><td colspan="3">公共基础</td><td>必修</td><td>45/11.5</td><td>908</td><td rowspan="13">51.9%</td></tr>
<tr><td colspan="3">素质拓展</td><td>选修</td><td>6/0</td><td>96</td></tr>
<tr><td rowspan="6">专业教育</td><td rowspan="3">专业课程</td><td colspan="2">学科基础</td><td>必修</td><td>18.5/1.5</td><td>296</td></tr>
<tr><td colspan="2">专业基础</td><td>必修</td><td>19.5/10</td><td>312</td></tr>
<tr><td colspan="2">专业核心</td><td>必修</td><td>16/10</td><td>256</td></tr>
<tr><td rowspan="3">专业分类培养</td><td rowspan="2">专业限选</td><td>数字内容安全</td><td>选修</td><td>6/3</td><td>96</td></tr>
<tr><td>艺术装备安全</td><td>选修</td><td>6/3</td><td>96</td></tr>
<tr><td colspan="2">专业任选</td><td>选修</td><td>4/2</td><td>64</td></tr>
<tr><td rowspan="4">实践教育</td><td>第二课堂</td><td colspan="3">创新创业综合训练实践</td><td>选修</td><td>8/8</td><td>160</td></tr>
<tr><td rowspan="3">第三课堂</td><td colspan="3">社会实践</td><td>必修</td><td>4 / 4</td><td>64</td></tr>
<tr><td colspan="3">专业实训</td><td>必修</td><td>16 / 16</td><td>256</td></tr>
<tr><td colspan="3">综合实践</td><td>必修</td><td>17 / 17</td><td>144+31 周</td></tr>
<tr><td colspan="6">合计</td><td>160 / 83</td><td>2652+31 周</td></tr>
</table>

（二）素质拓展课程体系设计

课程平台	课程类别	课程性质	学分	学时	开课学期	备注
通识教育	艺术+思政	选修	1-2	16-32	3-8	1.任选 6 学分，其中必选至少 2 学分公共艺术类课程； 2.“全人教育”依照四个学堂人生角色的核心培养目标，面向各年级递进式设置课程，分层次实施选课。
	艺术科技	选修	1-2	16-32	3-8	
	公共艺术	选修	1-2	16-32	3-8	
	人文素养	选修	1-2	16-32	3-8	
	基础技能	选修	1-2	16-32	3-8	
	安全教育	选修	1-2	16-32	3-8	
	体育与健康	选修	1-2	16-32	3-8	
全人教育	凤凰明理	选修	0.5-1	8-24	1-8	
	学堂明理	选修	0.5-1	8-24	1-8	
	凤凰博雅	选修	0.5-1	8-24	1-8	
	凤凰践行	选修	0.5-1	8-24	1-8	

十一、总体时间分配表

项目	学期	一	二	三	四	五	六	七	八	合计
1	入学教育、军训	3								3
2	教学周	16	16	16	16	16	16	16		112
3	考试周	2	2	2	2	2	2	2		14
4	毕业实习、毕业论文(设计、创作)								28	28
5	小学期	2		2		2				6
6	实践周		1		1		1			3
7	寒暑假	6	5	6	5	6	5	6		39
8	合计	29	24	26	24	26	24	24	28	205

注：单位周

十二、课程设置与教学进程

（一）通识教育课程教学进程表

课程代码	课程名称	课程性质	课程学分			课程学时			开课学期	开课周数	考核方式	备注
			学分	理论学分	实践学分	学时	理论学时	实践学时				
GGTS04081103	思想道德与法治 1	必修	1.5	1.5	0	24	24	0	1	12	考试	Y
GGTS04081104	思想道德与法治 2	必修	1.5	1	0.5	24	16	8	2	12	考试	
GGTS04082210	毛泽东思想和中国特色社会主义理论体系概论	必修	3	2.5	0.5	48	40	8	3	16	考试	
GGTS04082220	习近平新时代中国特色社会主义思想概论	必修	3	2.5	0.5	48	40	8	4	16	考试	S
GGTS04085300	马克思主义基本原理 1	必修	1.5	1.5	0	24	24	0	3	12	考试	
GGTS04086400	马克思主义基本原理 2	必修	1.5	1.5	0	24	24	0	4	12	考试	
GGTS04087100	中国近现代史纲要 1	必修	1.5	1.5	0	24	24	0	1	12	考试	Y/S
GGTS04088200	中国近现代史纲要 2	必修	1.5	1	0.5	24	16	8	2	12	考试	
GGTS04089200	形势与政策 1	必修	1	1	0	32	32	0	1-4	16	考查	
GGTS04089300	形势与政策 2	必修	1	1	0	32	32	0	5-8	16	考查	
GGTS04167101	大学外语精读 1	必修	2	1.5	0.5	32	24	8	1	16	考试	S
GGTS04167102	大学外语听说 1	必修	1	0.5	0.5	32	16	16	1	16	考查	
GGTS04168201	大学外语精读 2	必修	2	1.5	0.5	32	24	8	2	16	考试	
GGTS04168202	大学外语听说 2	必修	1	0.5	0.5	32	16	16	2	16	考查	
GGTS04169301	大学外语精读 3	必修	2	1.5	0.5	32	24	8	3	16	考试	

GGTS04169302	大学外语听说 3	必修	1	0.5	0.5	32	16	16	3	16	考查	
GGTS04160401	大学外语精读 4	必修	2	1.5	0.5	32	24	8	4	16	考试	
GGTS04160402	大学外语听说 4	必修	1	0.5	0.5	32	16	16	4	16	考查	
GGTS04161100	大学体育 1	必修	1	0	1	36	0	36	1	16	考查	
GGTS04162200	大学体育 2	必修	1	0	1	36	0	36	2	16	考查	
GGTS04163300	大学体育 3	必修	1	0	1	36	0	36	3	16	考查	
GGTS04164400	大学体育 4	必修	1	0	1	36	0	36	4	16	考查	
GGTS04166100	大学生人文素养 1	必修	1	1	0	16	16	0	1	8	考试	
GGTS04167200	大学生人文素养 2	必修	2	1.5	0.5	32	24	8	2	16	考试	
GGTS04168200	大学生心理健康教育	必修	2	1.5	0.5	32	24	8	1-2	16	考试	
GGTS04092301	创造性思维与创新方法	必修	1	1	0	16	16	0	1-2	8	考查	
GGTS04092302	大学生职业生涯规划 1	必修	0.5	0.5	0	10	10	0	1-2	8	考查	S
GGTS04092322	大学生职业生涯规划 2	必修	0.5	0.5	0	10	10	0	3-4	8	考查	
GGTS04092303	大学生创业实务管理	必修	1	0.5	0.5	16	8	8	2-3	8	考查	
GGTS04092315	大学生就业指导	必修	1	1	0	20	20	0	5-6	8	考查	
GGTS04168100	军事理论	必修	2	2	0	36	36	0	1-2	16	考试	
GGTS04168101	大学生国家安全教育	必修	1	1	0	16	16	0	1-2	8	考试	
合　计			45	33.5	11.5	908	612	296				

（二）专业课程教学进程表

课程	课程	课程	课程	课程学分	课程学时	开课	开课	考核	备注

类别	代码	名称	性质	学分	理论学分	实践学分	学时	理论学时	实践学时	学期	周数	方式	
学科基础课程	ZYTS08144101	高等数学Ⅰ	必修	3	3	0	48	48	0	1	16	考试	
	ZYTS08144102	大学物理	必修	4	3	1	64	48	16	1	16	考试	
	ZYTS08144203	高等数学Ⅱ	必修	3	3	0	48	48	0	2	16	考试	
	ZYTS08144204	线性代数	必修	2.5	2.5	0	40	40	0	2	16	考试	
	ZYTS08144305	离散数学	必修	2	2	0	32	32	0	3	16	考试	
	ZYTS08144406	概率论与数理统计	必修	3	3	0	48	48	0	4	16	考试	
	ZYTS08144507	学术论文写作	必修	1	0.5	0.5	16	8	8	5	8	考查	
	小计			18.5	17	1.5	296	272	24				
专业基础课程	ZYJC08144201	程序语言设计	必修	3	2	1	48	32	16	2	16	考查	X
	ZYJC08144202	数据结构与算法	必修	2	2	0	32	32	0	2	16	考试	
	ZYJC08144303	操作系统原理	必修	2.5	1	1.5	40	16	24	3	16	考查	
	ZYJC08144304	信息安全数学基础	必修	3	3	0	48	48	0	3	16	考试	
	ZYJC08144405	数据库系统原理及应用	必修	3	0.5	2.5	48	8	40	4	12	考查	
	ZYJC08144406	面向对象程序设计	必修	3	1	2	48	16	32	4	16	考查	Z
	ZYJC08144407	计算机网络	必修	3	1	2	48	16	32	4	12	考查	X
	小计			19.5	10.5	9	312	168	144				
专业核心	ZYHX08144101	网络空间安全导论	必修	1	1	0	16	16	0	1	8	考查	
	ZYHX08144302	应用密码学	必修	3	1	2	48	16	32	3	16	考试	Z

课程	ZYHX08144403	大数据安全	必修	4	2	2	64	32	32	4	16	考查	Z/S
	ZYHX08144504	网络空间安全法律法规	必修	1	1	0	16	16	0	5	8	考查	S
	ZYHX08144505	数字内容 AI 对抗防御	必修	3	1	2	48	16	32	5	12	考查	S
	ZYHX08144506	网络攻防技术与实践	必修	4	0	4	64	0	64	5	16	考查	Z
	小计			16	6	10	256	96	160				

（三）专业分类培养课程教学进程表

课程类别		课程代码	课程名称	课程性质	课程学分			课程学时			开课学期	开课周数	考核方式	备注
					学分	理论学分	实践学分	学时	理论学时	实践学时				
专业限选	数字内容安全	ZYXX08144501	人工智能原理	选修	2	1	1	32	16	16	5	16	考查	
		ZYXX08144502	数字艺术品加密与确权	选修	2	1	1	32	16	16	5	16	考查	
		ZYXX08144603	艺术内容数据安全防护与溯源	选修	2	1	1	32	16	16	6	16	考查	
		ZYXX08144604	数字图像处理	选修	2	1	1	32	16	16	6	16	考查	
		ZYXX08144705	隐私保护技术	选修	2	1	1	32	16	16	7	16	考查	
		ZYXX08144706	数字内容风险评估与审计	选修	2	1	1	32	16	16	7	16	考查	
	至少选修 6 学分				6	3	3	192	96	96				
	艺术装备安	ZYXX08144507	数据库安全	选修	2	1	1	32	16	16	5	16	考查	Z
		ZYXX08144508	物联网系统安全	选修	2	1	1	32	16	16	5	16	考查	
		ZYXX08144609	沉浸式艺术系统安全	选修	2	1	1	32	16	16	6	16	考查	
		ZYXX08144610	信息隐藏技术	选修	2	1	1	32	16	16	6	16	考查	

	全	ZYXX08144711	智能舞台设备安全管理	选修	2	1	1	32	16	16	7	16	考查	
		ZYXX08144712	智能终端与艺术设备安全	选修	2	1	1	32	16	16	7	16	考查	
	至少选修 6 学分				6	3	3	192	96	96				
专业任选		ZYXX08144625	艺术操作系统安全	选修	2	1	1	32	16	16	6	16	考查	
		ZYXX08144626	演出控制系统安全分析	选修	2	1	1	32	16	16	6	16	考查	
		ZYXX08144627	云渲染平台安全	选修	2	1	1	32	16	16	6	16	考查	
		ZYXX08144728	数据分析演练	选修	2	1	1	32	16	16	7	16	考查	
		ZYXX08144729	网络舆情分析	选修	2	1	1	32	16	16	7	16	考查	
		至少选修 4 学分			4	2	2	64	32	32				

（四）实践教学环节

课程类别	课程代码	课程名称	课程性质	课程学分			课程学时			开课学期	开课周数	考核方式	备注
				学分	理论学分	实践学分	学时	理论学时	实践学时				
实验实践	NLSJ08144201	行业调研	必修	1	0	1	–	–	–	2	1	考查	
	NLSJ08144402	Web 安全实践	必修	2	0	2	–	–	–	4	2	考查	
	NLSJ08144603	数据库安全实践	必修	1	0	1	–	–	–	6	1		
	小　　计			4	0	4	–	–	–		4 周		
实习实训	NLSJ08144603	企业实习	必修	2	0	2	–	–	–	6	2	考查	
	NLSJ08144604	密码学应用实训	必修	4	0	4	64	0	64	6	16	考查	
	NLSJ08144705	数字内容安全实训	必修	4	0	4	64	0	64	7	16	考查	
	NLSJ08144706	网络攻防技术实训	必修	3	0	3	48	0	48	7	16	考查	

	NLSJ08144707	信息安全综合实训	必修	3	0	3	48	0	48	7	16	考查	
	小　　计			16	0	16	224	0	224		2 周		
综合实践	CXCY04090008	创新创业综合训练实践	选修	8	0	8	160	0	160	1-8	-	考查	
	NLSJ04161000	军事技能	必修	2	0	2	112	0	112	1	3	考查	
	NLSJ04169400	劳动教育	必修	1	0	1	32	0	32	1-6	-	考查	
	NLSJ08143707	毕业设计	必修	8	0	8	-	-	-	7-8	16	考查	
	NLSJ04160004	毕业实习	必修	6	0	6	-	-	-	7-8	12	考查	
	小　　计			25	0	25	304	0	304	-	31 周		
合　　计				42	0	42	576	0	576		37 周		

备注：

1. 备注栏中的 Y 表示该课程为省级一流本科课程；Z 表示该课程为“专创融合”特色示范课程；K 表示该课程为跨校修读学分课程；S 表示该课程为课程思政示范课程，X 表示该课程为校企合作课程。

2. 专业课程中理论、实践 1 学分均按照 16 学时计。

6.教师及课程基本情况表

6.1专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
应用密码学	48	16	任亮	3
大数据安全	64	16	郭成	4
网络空间安全法律法规	16	2	杨雅媛	5
数字内容 AI对抗防御	48	16	刘娲萨	5
网络攻防技术与实践	64	16	徐剑	5
网络空间安全导论	16	2	薛楠	1
高等数学Ⅰ	48	16	于东明	1
大学物理	64	16	李博	1
高等数学Ⅱ	48	16	于东明	2
线性代数	40	8	任亮	2
程序语言设计	48	16	刘娲萨	2
数据结构与算法	32	16	兰梦常	2
离散数学	32	8	王全宇	3
操作系统原理	40	16	刘亚杰	3
信息安全数学基础	48	16	乔峰	3
概率论与数理统计	48	16	王卓禹	4
数据库系统原理及应用	48	16	陈廷斌	4
面向对象程序设计	48	16	杨景胜	4
计算机网络	48	16	任雪莲	4
学术论文写作	16	2	徐冰	5

6.2本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历毕业学校	最后学历毕业专业	最后学历毕业学位	研究领域	专职/兼职
陈廷斌	男	1974-11	数据库系统原理及应用	其他正高级	研究生	大连理工大学	管理科学与工程	博士	信息管理	专职
薛楠	男	1978-03	网络空间	其他副高	研究生	北京科技	计算机应	博士	网络安全	专职

			安全导论	级		大学	用技术		系统	
任亮	男	1982-04	应用密码学	其他正高级	研究生	东北大学	计算机应用技术	硕士	网络安全	专职
乔峰	男	1975-11	信息安全数学基础	副教授	研究生	北京工业大学	计算机应用技术	博士	信息安全	专职
任雪莲	女	1977-06	计算机网络	教授	大学本科	辽宁工程技术大学	机械工程及其自动化	学士	计算机应用	专职
刘亚杰	女	1982-08	操作系统原理	副教授	研究生	大连海事大学	计算机应用技术	硕士	软件工程	专职
杨景胜	男	1964-09	面向对象程序设计	副教授	研究生	大连理工大学	计算机应用技术	硕士	计算机程序开发	专职
徐冰	女	1987-12	学术论文写作	副教授	研究生	辽宁师范大学	计算机技术应用	硕士	计算机应用	专职
王全宇	男	1993-11	应用密码学	其他中级	研究生	辽宁工业大学	应用数学	硕士	网络安全	专职
刘娲萨	女	1987-09	程序语言设计	助教	研究生	韩国东义大学	影像叙事	博士	程序设计	专职
兰梦常	女	1998-09	数据结构与算法	助教	研究生	大连海洋大学	计算机应用技术	硕士	大数据	专职
于东明	男	1982-01	高等数学	讲师	研究生	辽宁科技大学	计算机技术领域工程	硕士	工程设计	专职
王卓禹	女	1999-11	概率论与数理统计	助教	研究生	大连交通大学	物流工程与管理	硕士	工程管理	专职
李杰	男	1979-07	网络攻防技术实训	副教授	研究生	清华大学	计算机科学与技术	博士	安全管理信息技术	专职
杨雅媛	女	1982-10	网络空间安全法律法规	副教授	研究生	北京工业大学	计算机软件与理论	硕士	信息网络安全监管	兼职
郭成	男	1980-01	大数据安全	教授	研究生	大连理工大学	计算机应用技术	博士	大数据安全	兼职
徐剑	男	1978-07	网络攻防技术与实践	教授	研究生	东北大学	计算机应用技术	博士	网安攻防对抗关键技术研究	兼职
李博	男	1988-12	AI安全	其他正高级	研究生	诺森比亚大学	计算机科学	硕士	AI视觉与AI识别	兼职

6.3教师及开课情况汇总表

专任教师总数	14		
具有教授（含其他正高级）职称教师数	6	比例	33.33%
具有副教授及以上（含其他副高级）职称教师数	13	比例	72.22%
具有硕士及以上学位教师数	17	比例	94.44%
具有博士学位教师数	7	比例	38.89%
35岁及以下青年教师数	3	比例	16.67%
36-55岁教师数	14	比例	77.78%
兼职/专职教师比例	4:14		
专业核心课程门数	20		
专业核心课程任课教师数	17		

7.专业主要带头人简介

姓名	乔峰	性别	男	专业技术职务	副教授	行政职务	无
拟承担课程	信息安全数学基础			现在所在单位	大连艺术学院		
最后学历毕业时间、学校、专业		2009年毕业于北京工业大学计算机应用技术					
主要研究方向		信息安全					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		2020年出版财务管理与金融创新，北京工业大学出版社 2015年发表一种可信移动终端仿真架构，电子科学技术 2010年发表Electronic Paper Panel Image Display Method，美国专利PCT：12/323,327					
从事科学研究及获奖情况		无					
近三年获得教学研究经费（万元）	0.0			近三年获得科学研究经费（万元）	320.0		
近三年给本科生授课课程及学时数	授课大学生计算机课程学时32 授课人工智能导论课程学时32			近三年指导本科毕业设计（人次）	0		

姓名	任雪莲	性别	女	专业技术职务	教授	行政职务	无
拟承担课程	网站开发设计、程序设计基础、电子商务平台开发			现在所在单位	大连艺术学院		
最后学历毕业时间、学校、专业		2001年毕业于辽宁工程技术大学机械工程及其自动化（本科） 2009年12月，大连海事大学，计算机应用技术（硕士）					
主要研究方向		计算机应用技术					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		1.基于能力为重的电子商务专业人才培养模式研究，教改项目，主持人，省级 2.基于跨校修读学分课程《程序设计基础》的混合式翻转教学模式研究与实践教，改项目，主持人，省级					
从事科学研究及获奖情		获奖：					

况	1.2017年获辽宁省“民办教育教学优秀论文”二等奖 2.2015年获得辽宁省高等教育学会与辽宁省职业技术教育学会联合开展的“创新创业教育”征文评选活动 优秀征文三等奖 3.2008-2009年度辽宁有职业教育优秀科研果成果 三等奖 科研立项： 1.2015年电子商务专业本科层次职业技术人才培养模式研究，科研项目，主持人，省级 2.2018年校企协同创新背景下创新创业教育评价体系和监测研究，科研项目，主持人，省级 3.2017年基于校企协同创新背景下高校创新创业人才培养质量评价体系构建研究，科研项目，主持人，省级 4.2021年“双一流”视阈下民办院校应用型人才培养质量提升研究，科研项目，主持人，省级 5.2012年大连智慧旅游公共服务平台应用价值研究，科研项目，主持人，省级 6.2017年“一带一路”战略背景下大连市跨境电子商务多层次协同发展体系构建及其状态测评，科研项目，主持人，省级 7.2019年以校企协同双主体深度融合促进大连创新创业人才培养对策研究，科研项目，主持人，省级 8.2023年双创视角下民办高校毕业生就业能力提升策略研究，科研项目，主持人，省级 9.2023年艺术职业院校创新创业教育与专业教育有机融合的实践研究，科研项目，主持人，省级

近三年获得教学研究经费（万元）	0.5	近三年获得科学研究经费（万元）	2.0
近三年给本科生授课课程及学时数	授课网站开发设计、程序设计基础、电子商务平台开发课程学时1500	近三年指导本科毕业设计（人次）	30

姓名	任亮	性别	男	专业技术职务	其他正高级	行政职务	无
拟承担课程	应用密码学			现在所在单位	大连艺术学院		
最后学历毕业时间、学校、专业	2009年毕业于东北大学 计算机及应用专业						

<table>
<tr><td>主要研究方向</td><td colspan="3">网络安全</td></tr>
<tr><td>从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）</td><td colspan="3">2020年-2021年横向课题：工控安全漏洞挖掘系统，博智安全科技股份有限公司
2021年-至今横向课题：工控安全蜜罐系统，博智安全科技股份有限公司
2022年-至今横向课题：DDS协议栈开发，奥特酷智能科技（南京）有限公司</td></tr>
<tr><td>从事科学研究及获奖情况</td><td colspan="3">无</td></tr>
<tr><td>近三年获得教学研究经费（万元）</td><td>0.0</td><td>近三年获得科学研究经费（万元）</td><td>550.0</td></tr>
<tr><td>近三年给本科生授课课程及学时数</td><td>授课人工智能导论课程学时32</td><td>近三年指导本科毕业设计（人次）</td><td>0</td></tr>
</table>

<table>
<tr><td>姓名</td><td>徐剑</td><td>性别</td><td>男</td><td>专业技术职务</td><td>教授</td><td>行政职务</td><td>副院长</td></tr>
<tr><td>拟承担课程</td><td colspan="3">网络攻防技术与实践</td><td>现在所在单位</td><td colspan="3">东北大学</td></tr>
<tr><td colspan="2">最后学历毕业时间、学校、专业</td><td colspan="6">2013年7月毕业于东北大学 计算机应用技术</td></tr>
<tr><td colspan="2">主要研究方向</td><td colspan="6">网安攻防对抗关键技术研究</td></tr>
<tr><td colspan="2">从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）</td><td colspan="6">2018年ESI高被引论文：Dynamic Fully Homomorphic Encryption-based Merkle Tree for Lightweight Streaming Authenticated Data Structures
中科院1区，领域TOP期刊IEEE Transactions on Industrial Informatics:Efficient and Lightweight Data Streaming Authentication in Industrial Control and Automation Systems
2013年出版格理论与密码学，科学出版社</td></tr>
<tr><td colspan="2">从事科学研究及获奖情况</td><td colspan="6">无</td></tr>
<tr><td>近三年获得教学研究经费（万元）</td><td colspan="3">50.0</td><td>近三年获得科学研究经费（万元）</td><td colspan="3">321.0</td></tr>
<tr><td>近三年给本科生授课课</td><td colspan="3">授课软件安全课程学时40 授课人工智能安全课程学时32</td><td>近三年指导本科毕业设</td><td colspan="3">0</td></tr>
</table>

程及学时数		计（人次）	

姓名	郭成	性别	男	专业技术职务	教授	行政职务	副院长
拟承担课程	大数据安全			现在所在单位	大连理工大学		
最后学历毕业时间、学校、专业		2009年毕业于大连理工大学 计算机应用技术					
主要研究方向		大数据安全					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		2024年中国计算机学会推荐A类top期刊：IEEE Transactions on Dependable and Secure Computing, vol. 21, no.2 pp. 746-763, 2024. 2024年中国计算机学会推荐A类top期刊：IEEE Transactions on Information Forensics and Security, vol. 19, pp. 207-220, 2024. 2020年中国计算机学会推荐A类top期刊：IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 1034-1044, 2020. 2021.中科院1区top期刊：IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 1948-1957, 2021. 2019.01-2022.12 国家自然科学基金面上项目—面向外包云的高维不确定数据密文相似搜索研究，国家自然科学基金委 2023.01-2024.12辽宁省应用基础研究计划—多数据源下基于同态密码技术的密文机器学习训练研究，辽宁省科技厅 2016.01-2018.12国家自然科学基金青年项目—多重云存储中数据安全审计方法研究，国家自然科学基金委					
从事科学研究及获奖情况		无					
近三年获得教学研究经费（万元）	119.0			近三年获得科学研究经费（万元）	118.0		
近三年给本科生授课课程及学时数	授课网络信息安全课程学时32			近三年指导本科毕业设计（人次）	0		

8.教学条件情况表

可用于该专业的教学实验设备总价值（万元）	237.6	可用于该专业的教学实验设备数量（千元以上）	135（台/件）
开办经费及来源	1.学校的教育事业收入，包括：学费、住宿费和其他教育事业收入； 2.科研事业收入，包括：通过承接政府、企事业单位横向课题；开展科研协作；转化科技成果、 提供科技咨询等取得的收入； 3.经营收入，指专业在教学、科研及其辅助活动之外，开展非独立核算经营活动取得的收入； 4.其他收入，例如：捐赠收入等。		
生均年教学日常运行支出（元）	4089.09		
实践教学基地（个）	5		
教学条件建设规划及保障措施	网络空间安全专业秉承学校“立足行业、课程为核、师资为翼、实训为桥、资源为链、平台为台”的建设理念，致力于在现有教育基础上实现学科建设跨越式发展。依托学校深厚的行业积淀与广泛的社会联系，强化资源整合，优化师资队伍，丰富课程体系，完善实训设施，与行业企业共建合作平台。目前，学校拥有两大校区，总面积达71.67万平方米，建筑面积38.2万平方米，教学设施及科研仪器设备先进，图书资源丰富。学校逐年增加教育投入，特设专业建设、师资引进与教师培训基金，继续优化教学环境，合理配置师资与资源，升级实验室设施以满足学科需求。提升教学投入，优化实训条件，规划资金使用，打造高标准智能交互设计专业。确保资源优先配置，保障教师与设备完备，确保新专业建设的顺利进行。智能交互设计专业携手数字媒体艺术、产品设计、园艺等专业，共同打造艺术科技学科集群。本校已建设辽宁省文化创意产业智库、大连数字文化产业发展研究基地在内等多个科研平台，配备了50余间先进的专业实训室，现有30家与专业紧密相关的校外实践教学基地供师生开展实践学习，以及总价值超过1400万元的教学设备，全力支持智能交互设计专业的教学与创新活动。		

主要教学实验设备情况表

教学实验设备名称	型号规格	数量	购入时间	设备价值（千元）
深信服出口网关	Sangfor AD-2280	1	2013	174.0
深信服上网行为管理	Sangfor AC-6080	1	2013	520.0
深信服SSl VPN	Sangfor VPN-2050	1	2013	58.0
深信服防火墙软件	AF-2000-B2150-SK	1	2021	50.0

深信服安全云脑	AF-2000-B2150-SK	3	2021	13.0
深信服VPN网关	AF-2000-B2150-SK	1	2021	8.0
VPN网关管理软件	VPN-1000-B1360-6C	1	2020	62.0
SSL VPN授权软件	V6.0	1500	2020	120.0
绿盟WEB应用防护系统	WAFNX3	1	2021	131.0
绿盟数据库审计系统	DASNX3	1	2021	67.0
绿盟安全管理系统	OSMSNX3	1	2021	57.0
绿盟安全评估系统	RSNX3	1	2021	95.0
惠普台式电脑	HP Elite Tower 680G9	110	2023	935.0
防火墙	DAS-TGFW-160	1	2024	20.0
态势感知系统	DAS-ABL-A690	1	2024	200.0
WAF防火墙	DAS-WAF-180AG	1	2024	40.0
运维审计系统	DAS-USM180	1	2024	50.0
日志审计系统	DAS-LOG-300-C	1	2024	55.0
数据审计系统	DAS-DBAuditor-1500C1	1	2024	56.0
终端防泄露	DAS-UES-HY	1	2024	45.0
智能密码钥匙	UKEY-RS	100	2024	5.0
动态口令令牌	MI2205V1	100	2024	10.0
动态口令认证系统	MI_SERVERV1.0.0	1	2024	150.0
签名验签服务器	DSVS-HG8001	1	2024	80.0
服务器密码机	HSM-A8001	1	2024	80.0
身份认证系统	DICA-A8001	1	2024	150.0
IPSec/SSL综合安全网关	CSG-A3001	1	2024	80.0

9. 申请增设专业的理由和基础

一、增设专业的主要理由

数字化转型的深入和新兴技术的应用扩大了网络攻击面，AI、云计算等技术的普及带来了全新的安全威胁，而《数据安全法》《关键信息基础设施安全保护条例》等政策法规的落地，推动企业在数据分类分级、跨境合规等领域加大安全投入。2024 年的《全球网络安全支出指南》显示，全球网络安全 IT 总投资规模有望在 2027 年增至 3288.8 亿美元；iiMedia Research 发布的数据显示，2024 年中国网络信息安全市场规模达 735.6 亿元，预计 2025 年可达 786.4 亿元，2027 年将达 884.4 亿元。

国家网信办数据显示，2025 年行业人才缺口已达 200 万人，较 2023 年增长 33%，尤其在漏洞挖掘、云安全等高端领域，仅 15% 从业者具备相关技能；《网络数据安全管理条例》等法规落地后，数据分类分级管理、跨境数据合规等细分领域新增人才需求超 50 万人。《网络安全人才实战能力白皮书》显示，到 2027 年我国网络安全人员缺口将达 327 万，而高校人才培养规模仅 3 万 / 年，企业对网络空间安全方向本科毕业生需求迫切且呈增长趋势。全国 1200 所左右理工科院校中，不足 45% 开办该专业；辽宁省虽积极推动网络安全产业园区建设和技术应用试点，但截至 2025 年 3 月，仅有 4 所本科院校开设该专业，远不能满足市场需求。

本专业的开设旨在深入贯彻《中国教育现代化 2035》，落实省委、省政府 “数字辽宁 智造强省” 部署，以建设一流应用型网络空间安全专业为目标，依托本地企业和业内领先行业，立足企业实际需求，走校企结合、产教融合的办学新路，保障网络空间安全人才培养与输送，顺应行业前沿发展趋势，切实满足企业实际需要。

二、支撑该专业发展的学科基础

大连艺术学院自2000年创建以来，经过19年的努力，学校逐渐发展成为艺术类综合门类协调发展，以培养艺术类应用型专业人才为办学特色的高等学府，已为国家培养各类毕业生5万余人。我校定位于“实践教学型”高等艺术院校，全面构建创新与实践教学体系，紧密结合社会人才需求，全面培养和提高各专业艺术人才的综合理论素养与实践能力，力争成为一所专业特色鲜明、办学成绩突出、在国内外具有一定影响的民办高等艺术院校。本专业深度依托学校在智慧校园、虚拟仿真及艺术科技领域的办学基础。智慧校园建设为网络安全实践提供了真实应用场景，虚拟仿真技术助力构建沉浸式攻防演练环境。同时，学校已成功申报智能交互设计和数字媒体技术专科工科专业，为网络空间安全专业的交叉融合发展奠定了工科教学基础，三者有机结合为网络空间安全专业打造了 “技术 + 艺术” 的跨学科培养土壤。

三、教学设施硬件建设：

学校已建成完善的实践教学平台，涵盖网络安全攻防实验室、数据安全分析中心、虚拟仿真实验基地以及艺术科技融合创新实验室。其中，网络安全攻防实验室配备下一代防火墙、入侵检测系统等专业设备；数据安全分析中心可支持 PB 级数据处理与加密测试；虚拟仿真实验基地基于 Unity 3D、Unreal Engine 等平台，构建 VR/AR 安全模拟场景；艺术科技融合创新实验室则聚焦智能舞台设备、数字艺术作品的安全测试，为学生提供从理论验证到产业应用的全链条实践环境。

四、师资队伍建设：

专业师资团队由校内骨干与行业专家组成，形成 “双师双能型” 教学团队。现有专职教师中，高级职称教师占比 62.5%，研究方向覆盖网络安全、软件工程、计算机程序开发、工程管理等领域。学校与华为共建大连首家人工智能 ICT 产业学院（计算方向），引入企业技术专家担任兼职导师，定期开展行业前沿讲座与项目指导；依托辽宁省 “艺术科技文化现代产业学院” 及教育部产学合作项目，教师团队深度参与企业实际项目，将华为云安全方案、腾讯内容安全审核系统等行业案例融入教学，确保课程内容与产业需求同步。

五、发展规划

网络空间安全专业的发展规划将从多维度推进，在现有基础上进一步拓展 “文化科技融合安全” 特色方向，计划增设《元宇宙场景安全》《文化遗产数字保护技术》等课程，针对元宇宙虚拟空间安全、文化遗产数字化过程中的数据安全等新兴领域开展教学与研究，强化专业在文化科技交叉领域的领先地位；同时持续深化与华为、深信服、奇安信等企业的合作，共建 “网络空间安全联合实验室”，联合开展智能内容审核算法优化、艺术科技设备安全标准制定等科研项目，推动 “订单式” 人才培养模式，根据企业需求定制课程模块，实现人才培养与产业需求的无缝对接；此外，积极开展国际合作办学，与欧美、日韩等网络安全领域领先院校建立合作关系，引入国际先进课程体系与教学资源，定期选派教师与学生参与国际学术会议、联合科研项目，提升师生国际视野与跨文化交流能力，打造具有国际影响力的网络空间安全专业品牌。

10. 校内专业设置评议专家组意见表

校内专业设置评议专家组意见表

<table>
<tr><td colspan="2">总体判断拟开设专业是否可行</td><td>☑是 □否</td></tr>
<tr><td colspan="3">理由：
校内专业设置评议专家组审阅了拟新增网络空间安全专业的申请材料，经充分评议，一致认为：网络空间安全专业的设立高度契合国家“网络强国”战略和“数字中国建设”战略，网络空间安全作为保障个人权益、社会稳定、国家主权与全球数字经济健康发展的核心基石，其设立能满足区域数字文化产业对安全人才的迫切需求，符合我校“十四五”学科专业建设规划及新工科发展要求，对优化我校学科布局、推动数字文化与网络安全跨学科融合，以及保障传统学科数字化转型安全具有重要战略意义。专业师资队伍结构合理，具备扎实的网络攻防、数据安全、密码学等领域的学术与工程背景。依托现有产业学院和实训基地，深化“校企合作、产学结合”实践模式，可充分满足该专业高强度攻防演练、安全系统开发与实践教学需求。
专家组认为，该专业人才培养方案目标清晰，课程体系科学完整，课程特色突出，并注重与法学、社会学等领域的交叉融合；方案强调实战能力培养，设置丰富攻防实验、安全实训及企业实习环节，与区域重点数字文化产业安全需求紧密结合。
经审议，专家组一致同意通过论证，建议将网络空间安全专业纳入学校 2025 年度拟新增本科专业名单，并按规定程序上报。</td></tr>
<tr><td colspan="2">拟招生人数与人才需求预测是否匹配</td><td>☑是 □否</td></tr>
<tr><td rowspan="3">本专业开设的基本条件是否符合教学质量国家标准</td><td>教师队伍</td><td>☑是 □否</td></tr>
<tr><td>实践条件</td><td>☑是 □否</td></tr>
<tr><td>经费保障</td><td>☑是 □否</td></tr>
<tr><td colspan="3">专家签字：</td></tr>
</table>

校外专家评审意见表

专业名称	网络空间安全

2025年7月7日，大连艺术学院组织相关专家针对学校网络空间安全专业筹建工作进行了评审。专家组审阅了相关申报材料，进行了现场考察，认真听取了学校汇报，经质询与讨论，形成意见如下：

1. 根据国家发展战略、产业人才需求及计算机类专业教学质量国家标准，专业精准聚焦知识产权保护、沉浸式艺术产品风险评估、艺术产品内容检测与防护三个方向，能够填补东北地区"AI+艺术+安全"应用型人才缺口。有效对接区域内文旅行业与东北艺术文化资源，对支撑辽宁数字创意产业集群升级具有战略意义。

2. 专业定位清晰，培养目标明确，毕业要求能够支撑培养目标，符合学校办学定位，能够充分利用现有关联专业优势，培养目标明确，毕业要求与课程体系相匹配，对学校跨学科建设具有重要意义。充分发挥科技对艺术全方位支撑和深层次推动作用，

3. 专业以学校现有 4 个省级现代产业学院与华为 ICT 产业学院为基础，并与深信服、奇安信等国内网络安全领域头部企业深度开展合作，现有教学条件、师资队伍、实践基地均符合《普通高等学校本科专业类教学质量国家标准》要求。课程设置合理，支持学生个性化发展。

专家组一致认为，大连艺术学院增设网络空间安全本科专业“定位契合国家战略和区域经济发展需要、基础条件成熟、培养方案特色鲜明”，符合国家对交叉学科建设的要求。同意申报该专业。建议进一步强化产学协同育人机制，开放实验室资源社会化服务，紧跟时代发展，强化办学特色。

专家组组长：徐剑

专家组成员：

许力 王丽 郭成 杨雅媛

2025年7月7日